Medical Big Data in Japan

By Yuichiro Tsuji

1. Abstract

Japan faces an aging society. The Japanese government is now deliberating how to provide Japanese people with medical services despite financial deterioration in the coming age. This paper focuses on one solution: the Medical Big Data Protection Act of 2018. In 2005, the Act on the Protection of Personal Information (APPI) took effect. This act was amended in 2015 to accommodate the big data era. It took effect on May 30, 2017. From the beginning, there was a strong objection to this act from doctors and hospitals. They argued that it would prevent and delay research and development. The Medical Big Data Act tries to resolve defects of the APPI to allow for medical use in an aging society. This paper uses constitutional and administrative law perspectives to review how Japan can efficiently and appropriately provide services in the coming age.

I. 2015 APPI AND CONNOTATIONAL AND ADMINISTRATIVE ISSUES IN JAPAN

The Statistics Bureau, under the Ministry of Internal Affairs and Communications, released that the current ratio of old age (over 65 years old) in Japan is 27.7 percent of the total population. The bureau predicts that number will be 35.3 percent in 2040. In comparison, the rate in the US is 15.4 percent. The Ministry of Health, Labor and Welfare (MHLW) estimates that the global average is 8.7 percent.[787] The drastically aging society in Japan is a priority of the Japanese government. The Japanese government implemented several measures to reduce the cost of medical coverage, such as a recommendation of exercise for metabolic syndrome.[788]

This paper focuses primarily on medical services and privacy issues. The Act on the Protection of Personal Information (APPI) was first established in 2003. It took effect in 2005.[789] APPI was revised in 2015[790], and the new version took effect in 2017. The purpose of the revision is to cover new privacy issues in the Japanese big data era. It aims to cope with the increasing possibilities of using personal data in a digital age

---

[787] Statistic Japan, Koreisha no jinko[Population of aging people](17, Sep, 2018). Available at: https://www.stat.go.jp/data/topics/topi1031.html

[788] Ministry of Health, Labor and Welfare, Heisei 28 nen Kokumin Kenko Eiyo chousa no kekka[Outcome of health ane nutirion of people](21, Sep, 2018).Available at : https://www.mhlw.go.jp/bunya/kenkou/seikatsu/06.html

[789] Act on the Protection of Personal Information, Act No. 57 of 2003 (Japan).

[790] Act on the Protection of Personal Information, Act No. 57 of 2003, Amendment of Act No. 65 of 2015 (Japan).

that demands the appropriate use of big data across national borders.[791]

As in the 2003 APPI, the 2015 APPI requires notification of the specified purpose for collecting user data, and prior consent of said person for third-party provisions. The first 2003 APPI defined these data as name, address, and date of birth. The 2015 APPI provides a new definition of personal information. Under the 2015 APPI, personal information means information relating to a living individual which falls under any of several items, such as name, address, and individual identifiers that enable one to identify a specific person.[792] These identifiers provide an easy reference to other information that can identify an individual.

The Personal Information Protection Commission (PIPC) publishes a guideline regarding this idea of "easy reference to other information". It "means that a business operator can easily reference other information by a method taken in the ordinary course of business".[793]

Personal identifier codes mean "certain types of data specified under a relevant cabinet order of the APPI, and includes biometric data which can identify a specific individual, or data in the form of a certain code uniquely assigned to an individual."[794] Examples of this type of information includes a person's fingerprints, facial recognition data, passport number, driver's license, and My Number.[795]

A. Japanese and US constitutional theory

Constitutional concern was raised about the protection of sensitive personal information. Since 1970, Professor Koji Sato and Tsuyoshi Hiramatsu[796] have argued that sensitive personal information was the most critical issue in Japan because it would lead to unjustifiable discrimination in society. They predicted that Japanese society may raise concerns regarding the abuse of extensional information. Without consent, small amounts of data about a person could be collected and used to create an individual image. Individuals would be alarmed if their data were collected without notice, and someone created his or her personal image from a mosaic of collected parts.

---

[791] Personal Information Protection Commission Japan, Outline of the amended Personal Information Protection Act (February,2016). Available at: https://www.ppc.go.jp/files/pdf/280222_outline_v2.pdf

[792] Article 2(2) of 2015 APPI.

[793] DLA PIPER, Data Protection Laws of the World, Japan (6, Oct., 2018).Available at: https://www.dlapiperdataprotection.com/

[794] *Id.*

[795] *Id.* My Number is the Social Security and Tax Number System in order to (1) enhance the social security to people who truly need it, (2) enhance public convenience and (3) develop the efficiency in administration.

Available at: https://www.cao.go.jp/bangouseido/foreigners/english.html

[796] Hiramatsu, Tsuyoshi, Jouhou koukai jourei no kaishaku [Interpretation of the freedom information ordinance],page108, 195 (Shinzansha 1998).

Sato, Koji, Praibashi-no kenri (sono kouhouteki sokumen) no Kenpo ron teki kousatsu [Constitutional analysis of public law phase of privacy right], Hougaku, Vol.86(1),page 1 (1970).

The element of "liberty" in the constitution means that we, the people, respect various ideas and ways of life as being dignified.[797] As humans, we may fear unrecognized perspectives and we may tend to suppress them. If we think we are being monitored by someone, we behave inconspicuously. This was called mosaic theory in the US Supreme Court case United States v. Jones.[798] In this case, the US Supreme Court held that it was illegal to use a warrantless Global Positioning System (GPS) device on a vehicle. In this case, concurring opinions were filed by Justices Alito and Sotomayor.

Justice Sotomayor argued that

> [p]eople disclose the phone numbers that they dial or text to their cellular providers; the URLS that they visit and the e-mail addresses with which they correspond to their Internet service providers; and the books, groceries, and medications they purchase to online retailers. . . . I for one doubt that people would accept without complaint the warrantless disclosure to the Government of a list of every Web site they had visited in the last week, or month, or year. But whatever the societal expectations, they can attain constitutionally protected status only if our Fourth Amendment jurisprudence ceases to treat secrecy as a prerequisite for privacy. I would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection.[799]

Justice Alito emphasized that

> if long-term monitoring can be accomplished without committing a technical trespass—suppose, for example, that the Federal Government required or persuaded auto manufacturers to include a GPS tracking device in every car—the Court's theory would provide no protection.[800]

Similar concerns regarding privacy were at the forefront of the majority opinion in Carpenter v. United States in 2018.[801] In this case, the US Supreme Court reviewed whether the location record of a mobile phone was protected by the Fourth Amendment. Justice Roberts wrote the majority opinion. He explained that technology raised concerns over protection of privacy. With newer technology, the government could enhance its "capacity to encroach upon areas normally guarded from inquisitive eyes, this Court has sought to 'assure preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted.'"[802]

---

[797] NIHON-KOKU KENPŌ [Constitution of Japan] May 3, 1947, preamble (Japan).

[798] United States v. Jones, 565 U.S. 400 (2012).

[799] Id. Sotomayor, J., dissenting.

[800] Id. Alito,J., dissenting.

[801] Carpenter v. United States, 585 U.S. ____ (2018).

This is analyzed in Tsuji, Yuichiro, GPS Investigations Under Constitution of Japan-Comparison with the US Cases (Sep 1, 2018). ICLR, 2018, Vol. 18, No. 1.pp.179-197. International and Comparative Law Review (Mezinárodní a srovnávací právní revue) . Available at SSRN: https://ssrn.com/abstract=3189947

[802] Id. at .

Justice Roberts confirmed that "an individual maintains a legitimate expectation of privacy in the record of his physical movements as captured through" a mobile phone.

Sato and Hiramatsu's concerns materialized in the decision of the US Supreme Court in 2018. In Japan, the 2015 APPI newly defined sensitive information to include race, creed, medical history, and personal information that has the potential to cause unjustifiable prejudice.[803] Obtaining sensitive information demands the consent of said person. It is desirable to require consent of the person for medical history because it may lead to unjustifiable discrimination. However, it may cause inefficiency and delay of medical research if consent requirements are too strict.

The 2015 APPI established wide exceptional use. To provide personal information to a third party demands the consent of the impacted person beforehand, but information may be provided without consent under the following exceptions:

> (i) cases based on laws and regulations, (ii) cases in which there is a need to protect a human life, body or fortune, and when it is difficult to obtain a principal's consent, (iii) cases in which there is a special need to enhance public hygiene or promote fostering healthy children, and when it is difficult to obtain a principal's consent, (iv) cases in which there is a need to cooperate in regard to a central government organization or a local government, or a person entrusted by them performing affairs prescribed by laws and regulations, and when there is a possibility that obtaining a principal's consent would interfere with the performance of the said affairs.

Even under the 2003 APPI, Hiramatsu argued that exceptions to the general rule would allow list brokers to abuse personal information for their profits.[804] Under the 2003 APPI, universities and hospitals used the above four exceptions when it was difficult to obtain the consent of an individual.[805]

The 2015 APPI clarified the requirement for prior consent for special care-required personal information such as race, creed, and medical history.[806] Medical record is not available without the consent of the impacted person. It is a good step in refraining list brokers. In the meantime, workers in medical fields may think that it is inconvenient for efficient use of medical data.

Universities and hospitals thought that the 2015 revision refrained medical doctors from performing medical research. The MHLW and PIPC have established guidelines to clarify abstract text that lead to interpretation issues in the 2015 APPI.[807]

---

[803] Art 3(2) of the 2015 APPI.

[804] Hiramatsu, Tsuyoshi, Kojin jouhou hogo [Datenshutzrecht],page 23,73,81,86,102-138(Yushindo 2009).

[805] Yuichiro Tsuji, Medical Privacy Issues in Ageing Japan (August 2, 2017). Australian Journal of Asian Law, Vol. 18, No. 1, article 6, 2017. Available at SSRN: https://ssrn.com/abstract=3012397

[806] Art 2(3) of the 2015 APPI.

[807] MHWL, Iryo kaigo kankei jigyosha ni okeru kojin joho no tekisetsuna toriatsukai no tameno gaidansu [Guideline for appropriate use of personal information in medical field](14, April, 2018).

Administrative regulations are helpful to cope with the interpretation of statutes in the face of rapidly developing technology. The parliament grants lawmaking power to agencies, but the legitimacy of those administrative agencies may be weaker than the parliament. Agencies can develop guidelines to clarify what an identifier is, such as a fingerprint.[808] The privacy law issue is moving far beyond a constitutional privacy discussion: it now concerns how people think sensitive information is being used in the medical services field.

B. DE-IDENTIFIABLE INFORMATION

The 2015 APPI set several regulations for the big data era. It incorporated the new notion of "de-identified information": any information about individuals from which all personal information has been removed when such removed personal information cannot be restored through measures specified in the enforcement rules and relevant PIPC guidelines.[809]

Under the 2015 APPI, it was very unclear whether "de-identified information" meant anonymized data or pseudonymous data.[810] The 2015 APPI aims to promote efficient use of data for various purposes by processing personal information to be de-identifiable. It prohibits users from restoring de-identifiable data to obtain original personal information. Under the 2015 APPI, it was unclear whether it was possible to recover personal medical data in the hospital by connecting anonymized data with other identifiers in a corresponding table. How to manage sensitive information was a big concern before the Diet passed the Medical Big Data Act in 2018.[811] The 2015 APPI defines sensitive information as special care-required personal information that includes medical history, data from medical checks, instructions from a doctor regarding a medical check, and prescriptions. During a hereditary examination, some incidental finding may be discovered and lead to discrimination or prejudice. Academic research in university hospitals is excluded under the 2015 APPI regulations, but university hospitals provide general medical services and conduct

Available at: https://www.ppc.go.jp/files/pdf/iryoukaigo_guidance.pdf.

[808] For analysis on law making power of legislature in Japan, Yuichiro Tsuji, Law Making Power in Japan - Legislative Assessment in Japan (October 1, 2016). Korean Legislation Research/10(1)/pp.173-204, 2016-10. Available at SSRN: https://ssrn.com/abstract=2987663 or http://dx.doi.org/10.2139/ssrn.2987663

[809] Art.36(1) of the 2015 APPI.

Cabinet Order to Enforce the Act on the Protection of Personal Information, Cabinet Order No. 28 of 2016, art.19.(Japan).

Mistsubishi Research Institute, Inc., Tokumei Kako jouhuo kojin jouhou no tekiseina rikatsuyou no arikatani kansuru doukou chousa[Report on appropriate use of anonymous information and personal information](March, 2018). Available at: https://www.ppc.go.jp/files/pdf/tokumeikakoujireisyu.pdf

[810] Yuichiro Tsuji, Medical Privacy Issues in Ageing Japan, Australian Journal of Asian Law, Vol. 18, No. 1, article 6, (2017).

[811] Medical Big Data Act on 12, May, 2018. Act. No. 28 of 2018 (Japan).

research. Separation of the two institutions (hospital and research facilities) in human resources is necessary for the management of personal information.[812]

Under the 2015 APPI, special care-required personal information requires prior consent from the individual. Business operators handling personal information have a duty to specify the purpose of utilizing the data and may not use it beyond the scope of what is reasonably considered relevant to the pre-authorized purpose.

II. MEDICAL BIG DATA ACT IN JAPAN

Before the Medical Big Data Act, it had been difficult for hospitals, universities, or research institutes to receive prior consent of individuals for sensitive data. The Medical Big Data Act was promulgated on May 12, 2017. Its purpose is to promote the advancement of new technology in the health and medical fields for the benefit of a long-living society. The government predicts development of artificial intelligence and internet technology in the medical field. More medical data would be stored for the invention of new medicines. The government hopes to keep people healthy and ensure high quality of life and medical services.[813]

The Medical Big Data Act makes it possible to use broadly sensitive data for medical research in a medical company, hospital, or university. It newly establishes obligations of a qualified "anonymously processed information handling business operator". A patient receives a medical exam or service in a hospital or research institute and receives advice from a doctor. Without consent of the patient, sensitive data is first transferred to a qualified anonymously processed information handling business operator, and may then be transferred to a research institute, university, or medical company. The patient reserves the right to refuse this transfer.

A. DIFFERENCES AND SIMILARITIES BETWEEN MEDICAL BIG DATA ACT AND APPI

The goals of improving medical services and maintaining a good health status among citizens could be easily sustained. The problems that remain are determining how this purpose can be achieved and preventing misuse and leakage of medical personal information. To identify issues within the Medical Big Data Act, it is helpful to see the differences and similarities between it and the 2015 APPI. Medical personal information is at the core of constitutional privacy. Thus, duties and responsibilities are outlined below.

---

[812] Yuichiro Tsuji, Medical Privacy Issues in Ageing Japan, Australian Journal of Asian Law, Vol. 18, No. 1, article 6, (2017).

[813] Prime Minister of Japan and his Cabinet, (11,May, 2018). Available at: https://www.kantei.go.jp/jp/singi/kenkouiryou/jisedai_kiban/houritsu.html

Similarities

First, Article 36(1)[814] of the APPI and Article 18(1)[815] of the Medical Big Data Act provide the duties of personal information handling business operators and certified operators "to process personal information in accordance with standards prescribed by rules of the Personal Information Protection Commission as those necessary to make it impossible to identify a specific individual and restore the personal information used for the production." They may not recover original personal information from anonymously processed information.

This is because Article 36(5)[816] of the APPI and Article 18(2) of the Medical Big Data Act require a personal information handling business operator and certified operator "to process personal information in accordance with standards prescribed by rules of the PIPC as those necessary to make it impossible to identify a specific individual and restore the personal information used for the production when they produce anonymously processed information."

Second, both a personal information handling business operators and certified operators have a duty not to collate "anonymously processed information with other information in order to identify a principal concerned with personal information used to produce the said anonymously processed information."[817]

Third, other personal information handling business operators and certified operators may create anonymously processed information. When other personal information handling business operators and certified operators want to use the information, neither of them shall "acquire information relating to those descriptions . . . or individual identification codes deleted from the personal information."[818]

Lastly, those professionals may each want to provide anonymously processed information to a third party. In such a case, both of them "shall, pursuant to rules of the Personal Information Protection Commission, in advance disclose to the public the categories of information concerning an individual contained in anonymously processed information to be provided to a third party and its providing method, and state to the third party explicitly to the effect that the information being provided is anonymously processed information."[819]

These similarities show that detailed and important regulations are drafted by the PIPC. The composition and power of the PIPC should be carefully reviewed from a constitutional privacy standpoint to ensure legitimacy.

---

[814] Art.36(1) of the 2015 APPI.
[815] Art.18(1) of the Medical Big Data Act.
[816] Art.36(5) of the 2015 APPI.
[817] Art.36(5) of the 2015 APPI.
Art.18(2) of the Medical Big Data Act.
[818] Art.38 of the 2015 APPI.
Art.18(3) of the Medical Big Data Act.
[819] Art.36(4), 37 of the 2015 APPI.

Differences

First, under the 2015 APPI, "[a] personal information handling business operator shall strive to keep personal data accurate and up to date within the scope necessary to achieve a utilization purpose, and to delete the personal data without delay when such utilization has become unnecessary." This is not a legal duty. Under the Medical Big Data Act, a certified operator has a legal duty to delete the data once utilization is no longer necessary.

Second, to comply with the rules of the PIPC, a personal information handling business operator shall take actions for the security control of data after producing anonymously processed information. This is not a legal duty. The Medical Big Data Act imposes a legal duty to certified operators to take necessary action for the security control of anonymously processed information.

Third, unlike a personal information handling business operator under the APPI, the Medical Big Data Act[820] clearly prohibits employees from disclosing and using medical and anonymously processed information for invalid purposes. Under the 2015 APPI, "[a] personal information handling business operator shall, in case of entrusting a whole or part of the handling of personal data, exercise necessary and appropriate supervision over an entrusted person so as to seek the security control of the personal data of which the handling has been entrusted." There is no limitation on the qualifications of this trustee. The Medical Big Data Act limits it to certified operators only.

Fourth, Article 23(1)[821] of the 2015 APPI allows third party provisions for cases based on laws and regulations. Article 23(2) allows a personal information handling business operator to provide personal data to a third party

> in cases where it is set to cease in response to a principal's request a third-party provision of personal data that can identify the principal and when pursuant to rules of the Personal Information Protection Commission it has in advance informed a principal of those matters set forth in the following or put them into a state where a principal can easily know, and notified them to the Personal Information Protection Commission, provide the said personal data to a third party notwithstanding the provisions of the preceding paragraph. (i) to set a third-party provision as a utilization purpose (ii) the categories of personal data provided to a third party (iii) a method of a third-party provision (iv) to cease, in response to a principal's request, a third-party provision of personal data that can identify the principal (v) a method of receiving a principal's request.

Article 23(2)[822] of the 2015 APPI requires that a personal information handling business operator shall notify a principal of these requirements or ensure that

[820] Art.22 of the Medical Big Data Act.
[821] Art.23(1) of the 2015 APPI.
[822] Art.23(2) of the 2015 APPI.

the principal can easily learn them. It is a very broad exception to the principle.

The Medical Big Data Act[823] demands only notification and carries no duty to put these requirements into a state where a principal can easily know them. The certified operator has a duty to report to the ministry, which has jurisdiction. The ministry has a duty to release it to the public.

Under the Medical Big Data Act, the term "medical personal information" is defined as a medical prescription that is a practitioners' receipt for a health insurance claim. The Diet seems to include medical questionnaires, medical examination results, and convalescence.[824] A committee discussed whether it may need reasonable time for a patient to claim a third party provision. The ministry established an ordinance to set a fixed time.

Under the 2015 APPI, a personal information handling business operator does not have a duty to provide paper documents to a petitioner. Contrary to this, under the Medical Big Data Act a certified operator does have a duty to provide paper documents to a petitioner.[825]

These differences show that the Medical Big Data Act has shifted the burden of control of personal data to the ministry and certified operators.

B. UNIQUENESS OF MEDICAL BIG DATA ACT AND DUTY OF HOSPITAL

Certified personal information handling business operators hand anonymously processed personal information to third parties such as medical companies or research institutes. They may research effects and efficiencies of medical treatments and propose more appropriate medical services for patients. Those involved in medical services are also expected to discover side effects of medications. Data sharing and safety comparisons across several institutions may be better and easier. In Japan, each hospital is specialized in general and may not be willing to share medical personal data. The Medical Big Data Act aims to share the anonymously processed information among several medical institutions so that more integrated evaluation may be available. Software to support comprehensive treatment using advanced technology may also be invented.

Under the Medical Big Data Act, original medical personal information may not be transferred without making changes to it. It should be processed in an anonymous format for research. To prevent misuse and leakage of data, personal information handling business operators are certified for safety management and control in processing. Their qualifications are reviewed periodically. Certified operators may provide data to a third party that is certified by the ministry. This

---

[823] Art.30(1) of the Medical Big Data Act.

[824] Kazuhiro Ohsima's statement in the Committee on Cabinet in the House of Councilors on 25, April. 2017.

Available at: http://kokkai.ndl.go.jp/SENTAKU/sangiin/193/0058/19304250058007.pdf

[825] Art.31 of the Medical Big Data Act.

certification works as a license.

A patient reserves the right to reject a third party provision. If the patient rejects a third party provision, anonymous medical information may not be given to the third party. The hospital does not have a duty to provide medical information to the third party. Data can be provided to a third party through a certified personal information handling business operator. If this occurs, the certified personal information handling business operator has a duty to notify the patient and report to the ministry. If a patient requests, the hospital needs to provide a document to stop third party provision and record a copy of that document. The hospital does not owe a legal duty to delete data that was already given to the third party. The hospital may be inspected by the ministry and may be required to present a report to the ministry.

One uniqueness of the Medical Big Data Act is that a hospital may provide medical personal data without consent of a patient unless he or she clearly objects. Under the 2015 APPI, anonymously processed information is not limited only to medical information. A person may not reject a third party provision under the APPI if it observes Article 23(2).[826]

Processing original data into anonymous data enables it to be used effectively. The Medical Big Data Act confines use of data to medical purposes because this type of data has a high possibility of being used for abusive purposes, such as unjustified discrimination. Under the 2015 APPI, personal information is able to be processed into anonymous information and is provided to non-certified persons. If this process is not thorough enough to secure data safety, heavier responsibilities may be imposed.

Under the 2015 APPI, original data and anonymously processed information for academic and research purposes are managed under the outlines provided in the Ethical Guidelines for Medical and Health Research Involving Human Subjects.[827] This third party provision is limited to research institute provisions.

The Medical Big Data Act alleviates a burden for hospitals because a certified personal information handling business operator processes original data into anonymous data. Certified operators are under strict management of the ministry. The success of the Medical Big Data Act depends on control of the government and how original data is processed into anonymous data. The Medical Big Data Act may have a disadvantage in that receivers of anonymously processed information cannot access the original data.

III. SUCCESS OF THE MEDICAL BIG DATA ACT

In general, people may not visit the hospital unless they get sick, and doctors in hospitals have copious patient data. If the purpose of the Medical Big Data Act is to

[826] Art.23(2) of the 2015 APPI.

[827] Ministry of Health, Labor and Welfare, Ethical Guidelines for Medical and Health Research Involving Human Subjects (March, 2015).Available at: https://www.mhlw.go.jp/file/06-Seisakujouhou-10600000-Daijinkanboukouseikagakuka/0000080278.pdf

secure the heath of the patient, constitutional privacy law would argue that the best interests of the patient is the priority. As Sato and Hiramatsu demonstrated, the general public in Japan has recognized that medical data are sensitive information that may lead to unjustifiable discrimination. As their perspective eventually showed, the success of the Medical Bid Data Act depends on the public's consciousness in Japan. The biggest concern is a vague sense of unease about the abuse of personal information. Constitutional analyses from the 1970s would be helpful to review when considering the Medical Big Data Act. If issues arise, past arguments may be helpful to predict the future. Uneasiness may suppress our liberty. The question is if we can find hope in the Medical Big Data Act.

Heavier burdens on anonymously processed information handling business operators may not be the perfect option. Its success depends on the feasibility of the business model. Privacy earns money and increases the cost. Information operators are managed by the government. The PIPC is comprised of privacy experts. Broad discretionary powers of the government might be twisted by political power or interested parties in establishment of regulations for the PIPC and licensing certification system. If the privacy business earns a large financial profit, it could be a lucrative field with a large clientele base.[828] Japanese people are not familiar with privacy law in Japan, with the exception of lawyers, and certification and licensing businesses related to privacy law requirements could grow to become a large industry.

Constitutional privacy law would argue that economic interest might be emphasized in the name of patient interest. In the meantime, obtaining prior consent in every case would prevent the development of medical research and services. For example, a patient may not be familiar with data use notices when they are seated in front of a doctor or visiting a hospital. Asymmetric information exits between a doctor and a patient.

We would be careful to promptly review the Medical Big Data Act that was recently established. The Ministry and PIPC could prepare guidelines and regulations soon.

The 2015 APPI established the PIPC in 2016. It is an "independent comprehensive supervising authority of personal information." Data protection used to be under the jurisdiction of competent ministries according to the field of business. Its authority moved to the PIPC. It should maintain a neutral composition, independent of business or political interests.

C. ETHICAL GUIDELINES FOR MEDICAL AND HEALTH RESEARCH

[828] From 2017 to 2018, the number of the APPI has been dramatically increasing. It was so difficult to translate provisions to English. European GDPR was not so familiar with Japanese people. Yuichiro Tsuji, Medical Privacy Issues in Ageing Japan, Australian Journal of Asian Law, Vol. 18, No. 1, article 6, (2017).

New York Times, Facebook Security Breach Exposes Accounts of 50 Million Users (29, Sep.,2018).Available at: https://www.nytimes.com/2018/09/28/technology/facebook-hack-data-breach.html

INVOLVING HUMAN SUBJECTS

In 2014, the Ministry of Education, Culture, Sports, Science and Technology and the Ministry of Health, Labor and Welfare jointly drafted the Ethical Guidelines for Medical and Health Research Involving Human Subjects. Its fifth chapter notes a procedure for informed consent of the patient. It raises that this guideline may conflict with the Medial Big Data Act. The government testified before the Committee on Cabinet in the House of Councilors on April 25, 2017.[829] The government explained to the committee that the ethical guideline was different from the act in that the ethical guideline targeted new medical treatments or testing new medicines on consenting patients. The Medical Big Data Act would use anonymized data from which it was impossible to recover personal information.

The government explained that the bill aimed to analyze data from existing medical research. They said that ex post facto research and statistical assessments were necessary to determine appropriate medical services and discover side effects of medications.

The government also explained that the Medical Big Data Act assigned duties to certified anonymously processed information handling business operators. The qualifications for the role require strict data security and the ability to process original data into anonymously processed data. After being certified, these individuals have a duty to maintain security measures. If they act in violation of the law, the government may conduct an inspection and issue a redress order. The government emphasized that it provided strict sanctions and would cancel certifications if those in this role do not obey the act. The government noted that qualified anonymously processed information handling business operators were under the management of the government, and patients would receive notice before transfer of data.

D. RISK ASSESSMENT

The Medical Big Data Act enables the use of personal medical data for various purposes. It inevitably involves risk assessment and safety measures. It incorporates risk assessment mechanisms: how widely medical anonymously processed information is used, the period of use, and continuity. If the system of processing personal information data into anonymous data is strict, the risk of re-identification will be small.

For example, a certified anonymously processed information handling business operator has several options. First, they may provide only a test outcome to a third party. Second, the third party should be qualified, which will ensure a high level of security. Third, they may give the data to a certified operator. Fourth, they may provide it to the public by processing the data widely. As the number of the people involved increases, the risk becomes more serious.

---

[829] Kazuhiro Ohsima's statement in the Committee on Cabinet in the House of Councilors on 25, April. 2017. Available at: http://kokkai.ndl.go.jp/SENTAKU/sangiin/193/0058/19304250058007.pdf

If the data has some continuity such as a medical history, the certified operator may process it by limiting the timeframe, applying a temporary identification code, and following strict protocol to transform the data. The data may be continuously provided to a particular institute. This may lead to easier reconnection between recent and old anonymously processed information through identifier codes. A certified anonymously processed information handling business operator may need to give a new temporary identification code every time, change the order of the record, and exclude any overlap period.

The Medical Big Data Act can take these protective measurements, but still faces some limitations of risk assessment. The Medical Big Data Act did not anticipate the worst-case scenario. Strict assessment would prevent efficient use of medical anonymously processed information. The certified operator has several options for third party provisions and ensures accountability.

Technology enables us to expand the use of anonymously processed information. Advances in technology may widen the possibilities of the current act and increase arbitrary use of that technology. Contrarily, old statutes could limit the advancement of medical information technology. The 2015 APPI was revised to cope with the big data era because previous policies did not address anonymous processed information.

Continuous review of the law is needed in the era of big data. New law may be required to promote the development of technology. That role is constitutionally assigned to parliament, the law-making organ. The executive branch fills a supplementary role in clarifying ambiguities in the text of statutes. In Japan, ministerial orders and guidelines written without legal power have played an important role in executing law. Administrative agencies are established by law and have both expertise and a democratic responsibility to voters. The judiciary reviews whether these agencies exercise their vested power arbitrary or capriciously. The judiciary is the last resort if defective statutes emerge in Japan because dispute over law is needed for jurisdiction.

E. US LAW AND MEDICAL BIG DATA

In the US, the Health Insurance Portability and Accountability Act (HIPAA) of 1996 is compared with the Medical Big Data Act in Japan. Their common concern is that anonymous information may be cross-referenced and recovered to original data.[830]

HIPAA provides policies, procedures, and guidelines for privacy. Its privacy rule sets requirements for identification such as name, address, and social security number.[831] Experts assess the risk of re-identification of individuals. Then, information is processed into de-identifiable data. HIPAA is a federal system in US, and state courts

[830] Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule, 45 C.F.R. §§160, 164 (2012).

[831] Id. § 164.514(b) (2014).Identifier under HIPAA is name, address, date, phone number, email account, social security number, etc.

may have differing privacy assessment regulations.[832] The Genetic Information Nondiscrimination Act (GINA)[833] also prevents unjustified discrimination in health insurance and employment. An insurer may not use genetic information to determine coverage, eligibility, or premiums.

The US Department of Health and Human Services (HHS) detailed administrative regulations for the de-identification of health information.[834] HHS defined de-identification of health information as a process that "does not identify an individual" nor provide "reasonable basis to believe that the information can be used to identify an individual."[835]

They further stipulate that

> A covered entity may determine that health information is not individually identifiable health information only if:
> (1) A person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable:
> (i) Applying such principles and methods, determines[836]…

As in Japanese law, US administrative agencies promulgate administrative regulations. It enables them to handle data flexibly and quickly in the face of rapidly developing technology. HIPAA and GINA suggest that it would be very difficult to remove all identifiers from original data. Research using that information may lead to the detection of other data regarding a person, such as relatives. Additionally, incidental findings may be discovered. Even though a patient provides consent, data may accidentally lead to negative possibilities for that patient's relatives. The rapid advancement of technology will lead to controversies beyond what legislators predict. Supplementary roles within administrative agencies and the judiciary would be expected to resolve these.

It is not clear if the Japanese Medical Big Data Act is managed appropriately by removing such risks, as in the US. Given this, we should revisit prior discussions regarding the right to privacy to ensure appropriate measures are in place.

2. CONCLUSION

This paper aims to review the Medical Big Data Act. The proportion of aging people is now increasing, and the government wants Japanese people to live healthy lives. It is constitutionally priority in Japan. Japan passed the Act on Protection of Personal Information in 2003. It aimed to strengthen the protection of privacy.

---

[832] 45 C.F.R. §§160, 164 (2012).

[833] Genetic Information Nondiscrimination Act (GINA) of 2008, Pub. L. No. 110-233, 122 Stat. 881 (codified as amended in scattered sections of 29 U.S.C. & 42 U.S.C.).

[834] Id. § 164.514(a).

[835] Id.

[836] 45 C.F.R.§§164.514(a), (b) (2009).

However, it could not handle big data flexibly. The revised APPI of 2015 makes it possible to use anonymously processed information for various purposes but makes it difficult for those who engage in medical work. This is because medical check results and medical histories are core to privacy. Knowledge of this data may lead to unjustified discrimination. The government has prepared some guidelines, without legal binding power, on how to apply the 2015 APPI in the medical field.

For example, under the 2015 APPI it is still possible to process original data into anonymous information for medical use. The 2015 APPI still demands that medical use of anonymous information requires consent of the person because it is a core of privacy. It has prevented the efficient use of medical information. With guidelines and administrative regulations, the 2015 APPI has a broad exception for third party provisions that are not available for medical use.

After these defects in the 2015 APPI were discovered, the Medical Big Data Act was established. It has both similarities and differences with the 2015 APPI. The personal information handling business operator and certified operator have a duty to make it impossible to identify a specific individual or restore anonymous information to its original data. They may not collate anonymously processed information with other information to identify a person.

Differences between the 2015 APPI and the Medical Big Data Act clarify the uniqueness of medical uses of personal information. Certified operators have a legal duty to maintain accurate information and to delete it after the stated purpose is achieved. Certified medical operators also have a legal duty to take necessary action to ensure security measures are in place. Employees are prohibited from disclosing and using medical data for invalid purposes. Only certified operators are permitted to be in the processing business. Certification requires a license from the government. This license is renewed periodically and certified operators may be inspected.

The Medical Big Data Act makes significant changes in the use of anonymously processed information for medical use. The anonymously processed information may be used without consent of the said person. The 2015 APPI was criticized for providing broad exceptions for third party provisions.

The success of the Medical Big Data Act depends on Japanese people. If unforeseen issues arise, we need to revisit past discussions to find a way to the future. The constitutional analysis that took place during the 1970s is helpful to understand today's situation. This is not unique to the future of the Japanese legal system. When we read US Supreme Court cases, the concurring opinions of Justice Sotomayor and Alito issued in the United States v. Jones case align with majority rulings of the US Supreme Court today.

The concept of "liberty" in the constitution means that we respect various ideas and ways of life. Humans may fear and suppress perspectives different from those we hold ourselves. When we believe we are being monitored, we behave differently. We should find hope, not fear, when we encounter different perspectives. This concept of privacy rights needs analysis of data collection if our eyes focuses on

technology too much. The most regulations for medical privacy are left to IPCC and administrative regulations. Japanese people don't recognize medical privacy is constitutional rights. The medical privacy business earns a large financial profit, and covered by name of economic right, not by autonomy or liberty. Japanese judiciary takes a role to define in concrete case what medical privacy is.

Federal statutes regarding medical services in the US address similar concerns as the Medical Big Data Act in Japan. These US documents are helpful in reviewing Japanese law. Even though strict responsibilities are mandated in statutes, the rapid development of technology may make it possible to abuse constitutionally vested governmental power and vice versa.

Cases involving incidental findings and anonymously processed information may test the Medical Big Data Act in the Japanese judiciary soon.