Advanced Biomedical Engineering
11: 48–57, 2022.

Original Paper

DOI:10.14326/abe.11.48

Data Processing Model for Compliance with International Medical Research Data Processing Rules

Yuki KURODA,[*, #] Goshiro YAMAMOTO,[*, **] Tomohiro KURODA[*, **]

Abstract In addition to traditional clinical research, advances in information communication technologies facilitates new medical research using internet of things devices and other cutting-edge technologies. Such medical research also simplifies the collection of data on research subjects in their daily lives internationally. In this context, medical research is increasingly required to comply with rules protecting patients' personal data. This study proposes a model to enable researchers and other stakeholders including ethics committees in such international medical research to easily verify whether the planned processing of patient data complies with relevant legal and ethical rules. The model proposed in this study consists of (1) how patient information is processed, (2) the rules that are relevant to the processing, and (3) the analysis of whether the processing complies with the rules. This study suggests that the model should describe the aspects of data processing that are subject to many rules, such as the location of the processing, categories of data, purposes of the processing, and the storage period. Thus, using the information described in the model as a guide, stakeholders can determine which national and international legal/ethical rules apply to the planned processing. Then, they can use the model to verify and document whether the processing complies with the specific regulatory rules. The use of the model in this study enables stakeholders in medical research to comply with the rules related to patient data more effectively than without using the model.

Keywords: data protection, privacy, data processing model, GDPR, regulatory science.

Adv Biomed Eng. **11**: pp. 48–57, 2022.

1. Introduction

This paper aims to reduce the burden on a research community regarding data processing rules from the perspective of regulatory science. Data processing in medical research, especially that leveraging internet of things (IoT) devices, has recently attracted great research interest. Several countries have adopted strict rules regarding sensitive participant information used in medical research. This is particularly relevant in international collaborative studies, in which multiple legal and ethical rules are generally applicable.

Some examples of such rules are as follows:

1. Personal data protection/privacy laws such as the General Data Protection Regulation (GDPR) [1] in the EU and the Act on the Protection of Personal Information (APPI) [2] in Japan;
2. Medical research rules such as the Common Rule [3] in the US; and
3. International ethical rules such as the World Medical Association's Declaration of Helsinki [4] and the Declaration of Taipei [5].

Compliance with multiple regulations and guidelines is a hurdle for many researchers. Several modalities have been proposed previously to help system designers plan data processing to comply with legal/ethical rules. Two categories of studies are relevant to our proposal. In the first category, some studies have previously proposed decomposing rules governing data processing into easily comprehensible formats for data users [6–8]. Such papers introduce algorithms and tables based on these decomposed rules and argue that these algorithms can determine the conditions which a given data processing activity should satisfy. In the second category, many data

This study was presented at the Symposium on Biomedical Engineering 2021, September, 2021.
Received on July 27, 2021; revised on October 29, 2021; accepted on December 20, 2021.

[*] Graduate School of Informatics, Kyoto University, Kyoto, Japan.
[**] Kyoto University Hospital, Kyoto, Japan.
[#] 54 Shogoin-kawahara-cho, Sakyo-ku, Kyoto 606–8507, Japan.
E-mail: yukikuroda@kuhp.kyoto-u.ac.jp

processing models have been proposed to enable appropriate data processing mainly at the design stage of information systems. They are affected by relevant concepts such as the Privacy by Design and Data Protection Impact Assessment [9–12].

The first category of research may be helpful if legal/ethical rules can be reduced to simple and straightforward algorithms. However, every rule involves vagueness and uncertainty in practical applications. Experts often encounter ambiguities in basic questions, such as whether a piece of information is classified as personal data under a particular rule. In addition, some ethical frameworks emphasize the importance of a stakeholder's input. Therefore, the legal/ethical decision-making process cannot be reduced to algorithms.

This study belongs to the latter category. The latter category of research aims to support human decision-making instead of replacing it. Previous studies in this group have attempted to incorporate legal/ethical concepts into models describing IT systems and data flows. The Data Protection Modeling Framework ("DPMF") makes an important contribution because it integrates data processing descriptions and legal concepts better than any other model [12]. DPMF is a model for describing data processing in compliance with the EU GDPR and is used in data protection impact assessment to assess the impact of planned data processing on individuals. However, as it only complies with the GDPR, it cannot be used for international data processing.

As discussed below, a model should distinguish facts related to the data processing (such as the purposes of processing and to whom the data is disclosed) from rule application (such as what conditions allow such data processing) in cases where multiple rules apply to the same data. However, the DPMF connects the facts of data processing and the application results, and it does not make a distinction. Furthermore, the DPMF also possesses constraints to ensure that the model description does not contradict the GDPR. However, some of the proposed constraints conflict with rules other than the GDPR. For example, the GDPR requires a legal basis for processing any kind of personal data [Article 6(1)]. In addition, the processing of special categories of personal data such as health data requires an additional legal basis [Article 9(2)]. The DPMF incorporates this legal structure and requires the user of the model to specify two legal bases for health data processing. However, even for health data, the APPI only requires one ground for processing. Thus, constraints of the DPMF prohibit the user from applying the model to data processing that is subject to the APPI.

It is worth noting that these problems are not unique to the DPMF. To the best of our knowledge, no previous study has described a case in which processing is subject to multiple legal/ethical rules.

Therefore, we propose a descriptive model for processing patient data in international medical research including clinical trials of medical devices. The proposed model is unique in the following aspects: (i) the facts underlying the application of the rules, (ii) the rules to be applied, and (iii) the application results. This enables a data processing model suitable for international medical research, which is subject to multiple data processing rules. We believe that our model can empower researchers and other stakeholders such as ethics committees to comply with multiple data processing rules.

2. Methods and Results

2.1 Study steps

This paper first examines the basic structure of applying legal and ethical rules, and then describes the features of international medical research in which data processing is subject to the personal data rules of several countries. Next, we present the basic structure of the proposed model in line with the features described and derive the elements of the model from the relevant rules.

In this study, we considered the following hypothetical case (**Fig. 1**).

2.2 Basics of rule application

We begin by clarifying how rules apply to the processing of patient data. The rules on data processing, i.e., the GDPR in the EU and the APPI in Japan, consist of two main layers. The first contains the conditions related to how data processing is subject to the rules. The second imposes specific conditions (such as specifying the purpose of use and obtaining consent) that regulate actual data processing activities. It is worth noting that the Declaration of Helsinki, a widely accepted ethical rule, has a two-tier structure. Even though it does not limit the geographical scope of application, the Declaration of Helsinki only applies to medical research that is conceptually distinguished from treatment.

Therefore, to apply a rule to processing, it is first necessary to determine which rule is applicable (the first layer) and then to state the specific conditions relevant to the given data processing within the applicable rule (the second layer). Both the first- and second-layer application processes have the same analysis process, as follows:

1. Identification of the applicable rules/conditions
2. Specification of the relevant facts
3. Application of the rules/conditions to the facts.

First, we begin with the first layer. Each rule on patient data defines its scope of application based on cer-

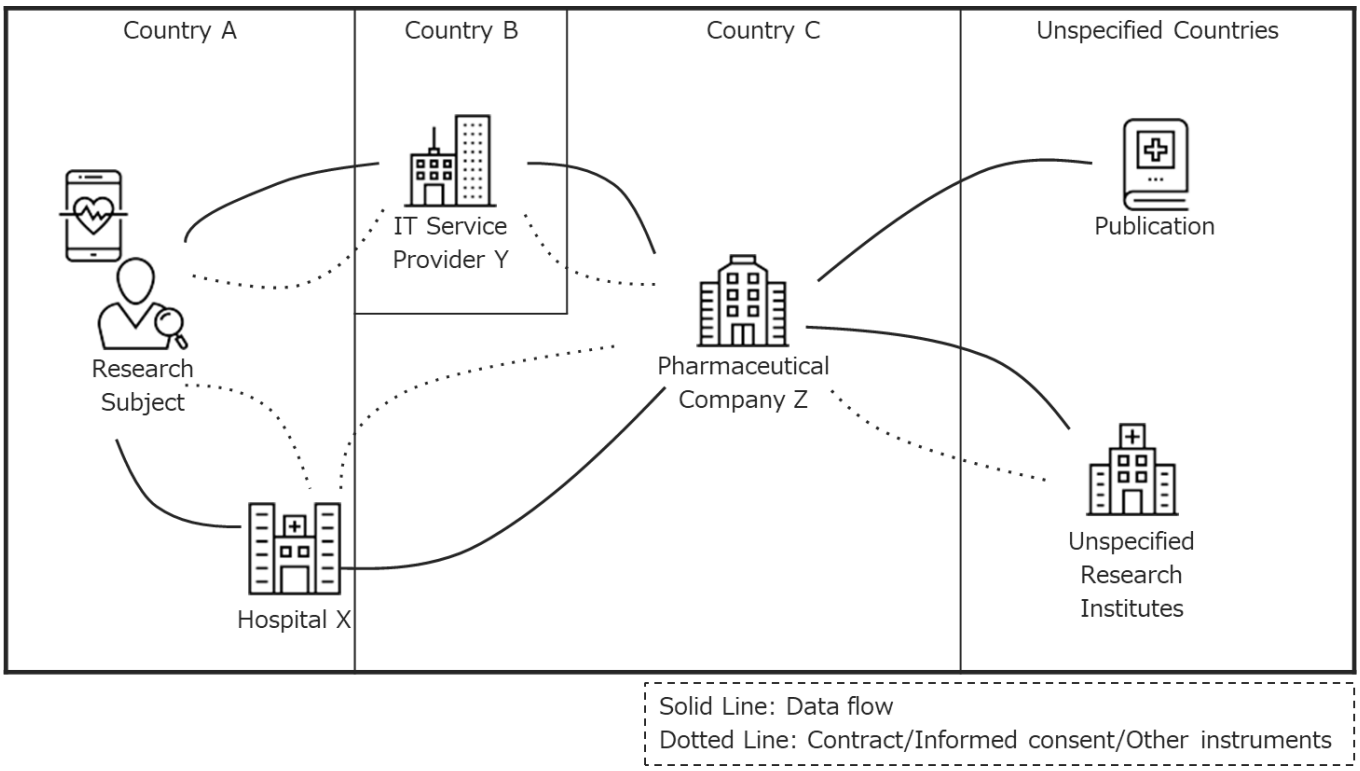

Fig. 1 A hypothetical case to be discussed in this paper. Research Subjects affected by a disease reside in Country A. They regularly visit Hospital X in the same country to receive treatments and examinations following a research protocol, and wearable devices are used to observe their home health status. The device data are transferred to an IT Service Provider Y located in Country B. The data collected by Hospital X and IT Service Provider Y flow to the Pharmaceutical Company Z in Country C, and X, Y, and Z collaborate in the research. X, Y and Z may publish the results of research in a journal. Z may also disclose the data to unspecified research institutes for secondary research. The journals and the institutes cannot be identified at the start of the study, so the countries where they are located are unspecified.

tain elements that include the location of a user and data subject, the type of data, and the purpose of processing. As each rule determines the corresponding scope of application independently, data processing may be subject to more than one rule.

A clear example is the processing of subject information by Z in the hypothetical case. We assume that the laws of Country C, where Z is located, apply to data processing by entities located in Country C. This assumption is in line with the rules of several countries. In addition, since Z monitors research subjects in Country A and collects data from outside Country A, the rules of Country A may apply to Z.

Furthermore, the data collected by Y through wearable devices are transmitted to Z for joint research. In this case, the rules of Country B, where Y is located, may oblige Z to comply with the same rules. However, this application is somewhat confusing. When data are exchanged between countries, the rules of the country in which the exporter is located may ensure the same level of protection after cross-border transfers. For this, the laws often oblige exporters to enter into contracts with the importers. As a result, in our scenario, Z is subject to the rules of Country B indirectly through a contract with Y, as well as the rules of Countries C and A. Considering ethical principles, Z may be obliged to follow the Declaration of Helsinki and other international ethical rules. Therefore, a model describing international medical research must be able to handle such situations.

We then moved to the second layer. The rules determined by the above process comprise a number of detailed conditions (clauses or provisions). Therefore, the analysis of the second layer also involves the following process:

1. Identification of the applicable conditions
2. Specification of the relevant facts
3. Application of the conditions to the facts

For example, rules such as the APPI in Japan and the GDPR in the EU require a personal data user to specify the purpose of processing. To apply this condition, the purposes proposed by a researcher must be identified as relevant. Then, stakeholders must check whether the proposed purposes are sufficiently specified from the perspective of each rule. Because different rules have differ-

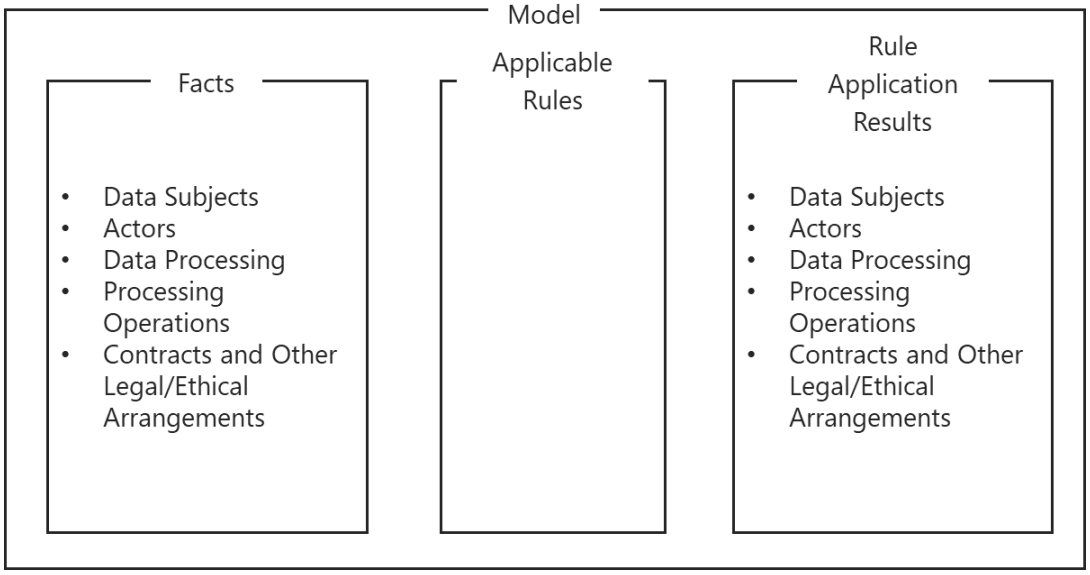

Fig. 2 Basic structure of the proposed model. The entire model comprises three major parts: Facts, Applicable Rules, and Rule Application Results. Facts and Rule Application Results are further divided into five subparts: data subjects, actors, processed data, processing operations, and contracts and other legal/ethical instruments.

ent standards, the proposed purposes specified for a rule may be deemed unspecific under another rule.

The legal/ethical rules on data processing established by national and international bodies include various conditions. In addition, some ethical frameworks list factors to be considered for ethical decisions, but do not set out clear conditions. Nevertheless, it is possible to derive essential elements from many rules regarding data processing. This is because rules influence each other, and some influential rules such as the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data often guide other rules. For instance, specifying the purpose of processing appears in the OECD Guidelines and other influential rules.

We argue that this interdependency of rules enables us to extract several conditions, which we often observe in many rules. However, this does not mean that our model can incorporate the specific conditions set out by all rules. A model user is free to extend the model as long as such an extension does not contradict the basic structure of the model.

2.3 Description of the model structure

Based on the above two-layered structure of rule application, the basic structure of the proposed model is as follows (**Fig. 2**).

To reflect the fact that multiple rules may be applied to the same processing, the model has a specific part of Applicable Rules. Furthermore, every rule application result is linked to a certain applicable rule.

The subparts in the Facts part and Rule Application Results part are defined as follows. Data subjects refer to the individuals whose data are to be processed, while actors refer to institutions, companies, and research organizations involved in medical research. The actors perform data processing operations. This subsection describes the purpose of processing, retention period, and third-party disclosure. The object of the processing operations is processed data. Processed data cover items in a dataset with granularity (individual-level or aggregated). Finally, contracts and other legal and ethical instruments mainly cover instruments among entities regarding data processing, such as joint research agreements between institutions and permissions from regulatory bodies. **Tables 1 and 2** describe items in the Facts part and Rule Application Results part.

Fig. 3 shows the relationship between the elements of the Facts part and Rule Application Results part.

It should be emphasized that previous studies regard IT systems as an essential component of the data description models. However, we focus on the actors, instead of IT systems, which process data. This is because legal and ethical rules impose obligations on entities that process data.

2.4 Description of detailed elements in the model

All subparts have certain items related to one or more conditions. As described above, such conditions originate from the relevant rules.

The items listed in the Facts part have different relations with the Rule Application Results. Some items in the Facts part have a straightforward relationship with

Table 1 Elements of the Facts part of the proposed model.

	Facts	Notes
Data Subjects	Category of research subject	
	Habitual residence	Related to applicable law
	Age of data subjects	Necessary to determine
	Supplemental attributes	Some rules deem several social or ethnic groups such as pregnant women or prisoners as vulnerable and offer special protection for them. Related facts are noted.
Actors	Name of an entity or the category of entities	Examples of categories: regulatory authorities, public research institutes, and private life-science companies
	Responsible person	A person in charge of data processing in an actor
Processed Data	Categories of data subjects	Data subjects of a given dataset
	Dataset name	Example is case report.
	Items in a dataset	Items in a given dataset
	Individual-level/aggregated data/statistics	Note: individual-level data may include individual-level anonymous data. This item does not imply linkability of data with a data subject.
	Whether the dataset contains a direct identifier	Necessary to check whether given data falls within personal data or similar concepts under a certain rule.
	Whether other datasets, including original data, can be collated with a given dataset	Same as above.
	Linkability with other datasets	Same as above.
Processing Operations	Purposes of processing	
	Processing manner	Processing includes disclosure, storage, alternation, and various other manners.
	Name of a third-party recipient or the category of a third-party recipient	Corresponding to the actors subpart.
	Specified/Unspecified	If the actors are described as a category, it must be unspecified.
	Established country/region	Country/region where an actor is established.
	Specified/Unspecified	If the actors are described as a category, it may be unspecified (i.e., domestic and foreign regulatory authorities)
	Conditions of a third-party disclosure	An example is additional approval by an ethics committee
	Retention period/condition	Planned retention period/conditions on the period
Contracts and Other Legal/ Ethical Instruments	Name of the arrangement	
	Parties in the arrangement	
	Nature of the arrangement	General description of the arrangement

the corresponding objects in the Rule Application Results part. Examples include the purpose of processing and third-party disclosure. Many rules require a data user to specify these items, and researchers can state them based on their research plan. However, even these items need to be examined under the conditions set by the rules. For example, many rules require that the purposes of use be specific. As noted earlier, whether the purposes identified by the researcher are sufficiently specific according to the standards set by the rules should be determined during rule application. Similarly, in medical research, a third-party recipient of the data may not be identified at the time of ethical approval. Whether a researcher is allowed to collect the data despite the uncertainty of a future recipient depends on the conditions set by the rules. Therefore, even for these simple items, the

Table 2 Elements of the Rule Application Results part of the proposed model.

	Rule Application Results	Notes
Data Subjects	Vulnerable group	Whether certain research subject group is given special protection under an applicable law
Actors	Fulfillment of requirements for responsible persons	Some rules such as the GDPR require an actor to designate a responsible person and specify his/her qualification.
	Representative	Some rules such as the GDPR require an actor to designate a representative in case the actor is located outside the territory of the rule (under the GDPR, an actor outside the EU may be required to designate a representative in the EU.).
Processed Data	How a given dataset is classified in light of the identifiability of a data subject	Which category the given dataset is classified into under certain rule (i.e., personal information, personal data, personally identifiable information, anonymous data)
	How a given dataset is classified in light of the content of data	Many rules offer special protection to sensitive data such as health data. Furthermore, certain health data such as genome data and sexually transmitted disease data may be given stronger protection than normal health data. Such special protection should be noted.
Processing Operations	Whether the purposes of processing are sufficiently specified	Many rules require that the purposes of processing are sufficiently specified.
	Classification of an actor processing data	Many rules classify actors into at least two categories. One is an actor who processes data for its own purpose and decides the manners of processing (some rules call actors of this type "controllers."). The other is an actor who processes data on someone else's behalf (often called a "processor."). This affects an actor's powers and obligations.
	Legal/ethical basis of processing	Many rules require a specific basis for data processing. A typical example is consent.
	Legal/ethical basis of cross-border transfer	Many rules require a specific basis for cross-border transfer. A typical example is consent.
	Whether recipients and the countries to which they belong are sufficiently specified	In particular, when the recipients are described as a category, a rule may interpret such a description ambiguous.
	Whether disclosure of data is permissible under a rule	Certain rules prohibit or set special conditions of international data disclosure.
	Obligation of record keeping	Many rules require an actor to keep relevant data for a certain period.
Contracts and Other Legal/ Ethical Instruments	Data processing arrangement	Whether an arrangement satisfies the requirements of an outsourcing arrangement.
	Cross-border arrangement	Whether an arrangement satisfies the requirements of a cross-border arrangement.

model needs to include these items both in the Facts part (planned purpose of processing) and in the Rule Application Results part (whether the planned purpose complies with the given conditions).

Not all items have simple relationship, such as the facts necessary for evaluating which categories the data will be classified under a particular rule. Each rule regulates a different range of data under different names, such as personal data and personally identifiable information. Therefore, how a given piece of data is categorized is entirely dependent on the rules. Thus, the model must distinguish between the facts necessary to conduct such analyses (whether data are categorized as personal data under the GDPR) and the result of the analysis (the data are not personal data). An identifier or linkability with the original data are examples of such facts.

As the model covers a wide range of legal/ethical rules on data processing, it should also include statistics and aggregated data even though many rules are only concerned with personal data or other similar concepts.

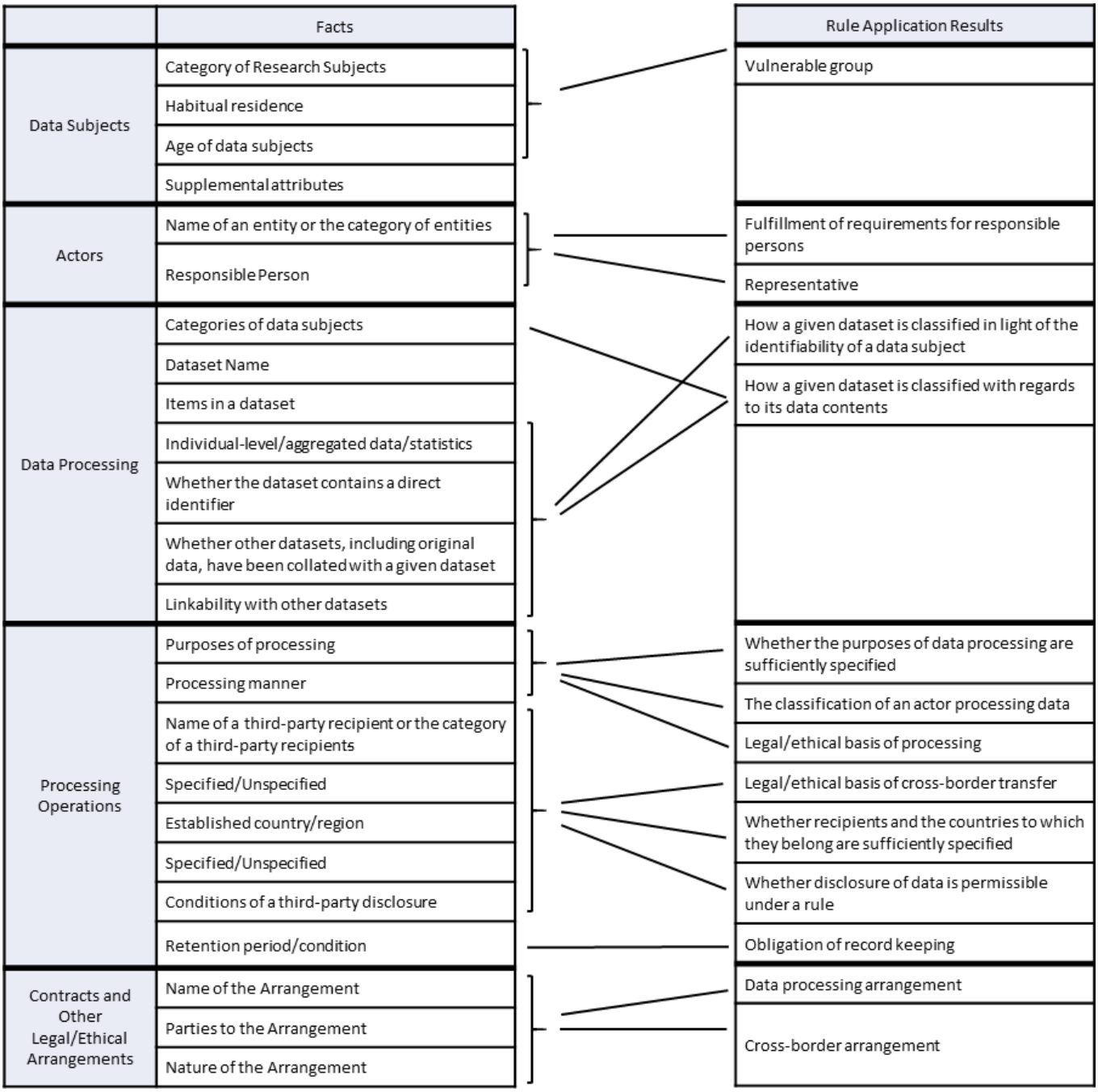

Fig. 3 Relations between the elements of the Facts part and Rule Application Results part.

This is because some ethical rules raise concerns about publishing results on geographical, ethnic, and racial groups.

The items listed in the proposed model were extracted from conditions frequently appearing in several rules. The rules used in the extraction process are listed in **Table 3**. As described above, the model does not consider all the conditions contained in these rules.

Note that Good Clinical Practice is not included because it sets out few specific conditions for processing research subject data other than maintaining confidentiality. Instead, we referred to the international ethical guidelines of biobanks, because they have more detailed provisions on data processing.

When extracting items from the referred rule, we mainly focused on the following:

1. Applications of the rules.
2. Data protection/privacy principles established by the rules.
3. Items that the rules require to be recorded.
4. Matters that the rules require to be informed to data subjects.

Item 1 relates to the first of the two layers, and items 2 to 4 relate to the second layer of the two-tier structure.

Table 3 Relevant rules for extracting the proposed model.

International	OECD, Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data [13]
	ISO, ISO/IEC 29100 [14]
	WMA, Declaration of Helsinki, Ethical Principles for Medical Research Involving Human Subjects [4]
	WMA, Declaration of Taipei on Ethical Considerations Regarding Health Databases and Biobanks [5]
	WHO IRAC, Common Minimum Technical Standards and Protocols for Biobanks Dedicated to Cancer Research [15]
	CIOMS, International Ethical Guidelines for Health-related Research Involving Humans [16]
	GA4GH, Framework for Responsible Sharing of Genomic and Health-Related Data [17]
Japan	Act on the Protection of Personal Information [2]
	Ethical Guidelines for Life Science, Medical and Health Research [18]
EU	General Data Protection Regulation [1]
US	Common Rule (45 C.F.R. 46) [3]
	HIPAA Privacy Rule (45 C.F.R. 164) [19]

Therefore, the proposed model does not include certain conditions in a target rule. A typical example of what the model does not cover is information security. This is because data processing description models dedicated to ensuring information security have already been proposed, and the rules referred to in this article often do not contain detailed conditions for information security.

3. Discussion

In this paper, we describe data processing in international medical research and propose a model to aid researchers in complying with data protection/privacy rules. The model is better than the DPMF because it can handle situations where multiple rules apply.

This basic model can be implemented in several scenarios and used to devise several specific methods of implementation. We use a hypothetical example to elucidate the application of our model.

Our implementation proposal consists of a flow-chart and tables. The flow-chart describes the basic relationship among a data subject and actors. As shown in **Fig. 1**, the relations among the actors are represented by solid and dashed lines. The solid line denotes the flow of data, and the dashed line indicates a relationship between entities, such as a contract. The flow-chart helps represent the entire data processing operation and can be used for basic analysis to find applicable rules. For example, assuming that Country A is the EU and Country C is Japan, Company Z is subject to at least the GDPR and the APPI (in reality more rules may apply to the processing at Company Z, such as the Japanese Ethical Guidelines, but we do not discuss these for simplicity). In this case, Z is the center of the research and processes the data received from X and Y. Z will publish the research results and make secondary use of the data obtained from the study in the future.

Compared with the flow-chart that describes inter-actor relationship, the tables provide more detailed processing information per actor. The tables follow the basic structure of the proposed model and include the parts on Facts, Applicable Rule, and Rule Application Results. We show an example of the table (**Fig. 4**).

Even though the GDPR and the APPI both use the same word; personal data, the definition in the GDPR is wider than that in the APPI. However, the data received from X and Y are likely to be personal data under both rules, at least during the duration of the research. By contrast, there may be differences between the two rules regarding specific processing conditions. For example, under both the APPI and the GDPR, such data can only be processed if a user has an appropriate legal basis. Under the APPI, processing is based on the consent of the subjects, whereas under the GDPR, the document issued by the European Commission [20] provides several potential legal bases. It states that consent cannot be the basis for processing in many clinical studies. Alternatively, in this example, we selected legitimate interest and scientific research as the legal basis. Thus, the model allows for a straightforward comparison of applying multiple rules to the same process.

By combining the flowchart and the tables described above, it is possible to describe the flow of data from a research subject to the publication of the final research results and the future possibility of secondary use of pseudonymized data at individual level.

We also suggest a scenario in which the model can

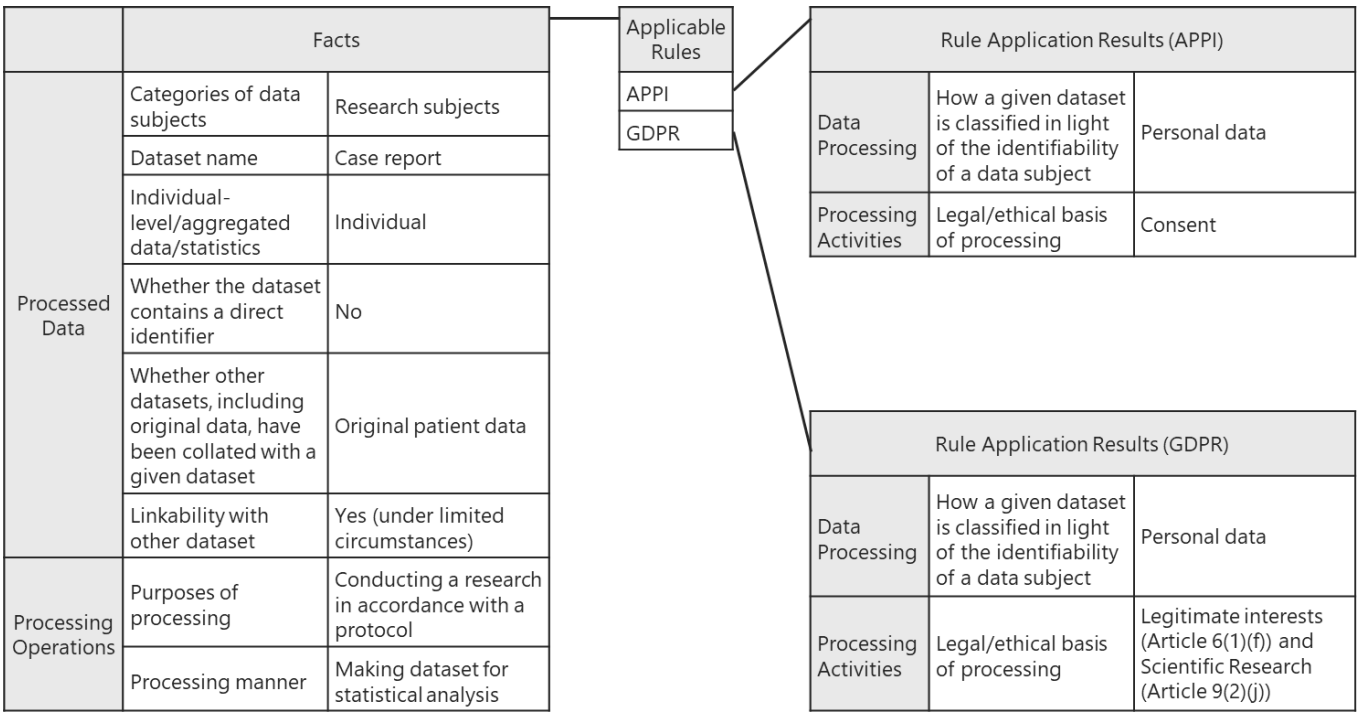

Fig. 4 Implementation example based on the hypothetical case. This small example contains the table component describing the internal data processing at Company Z.

be used. We envisage a step-by-step use of the model by stakeholders in medical research. First, a researcher fills in the Facts part related to processing while drafting a research protocol. Then, with the help of legal and ethical support staff, the researcher decides on the applicable rules and makes a provisional assessment based on the rules applied. In addition, the model together with the research protocol and an informed consent form (ICF) will be reviewed by an ethics committee. The committee is expected to use the research protocol and the ICF as a reference to validate the assessment. In addition, the model could be used in the course of actual research to verify the accuracy of periodic reporting, auditing, and monitoring.

It should be noted that this model will not impose additional burden on the researcher. As the above scenario shows, this model decomposes the entire compliance analysis process into several steps. Furthermore, it distinguishes the stage that the researcher can perform by himself from the steps where it is appropriate to seek other experts' help to complete. By this distinction, the researcher's task is mainly limited to fill in the Facts part. As **Table 1** shows, the items in the Facts part are fundamental aspects of data processing, and they should have been clarified during protocol drafting. Therefore, the researcher does not need to conduct additional analysis to fill in the model.

Our model allows extensions. As previously explained, if a relevant rule has a rare condition in data processing, it can be incorporated into the proposed model following the basic structure. Furthermore, the model can be extended to cover the processing of biospecimens in addition to patient data. This is because the rules for processing biospecimens obtained in research address similar issues such as the purpose, manner of use, and duration of storage.

The present study has some limitations. First, as in previous studies such as the DPMF, a stakeholder has not evaluated the proposed model. In addition, the proposed model has not been incorporated into software. It is necessary to adapt the proposed model into a system that is easy for stakeholders to use in the future.

4. Conclusion

This study introduces a new descriptive model for data processing in international medical research for compliance with patient data rules. The model reduces the burden on researchers and other stakeholders in complying with multiple data protection/privacy requirements.

Conflicts of interest

None declared.

Acknowledgement

Not applicable.

References

1. European Parliament and Council of the Europe Union: 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 (General Data Protection Regulation), 2016.
2. Government of Japan: The Act on the Protection of Personal Information, 2021 (last amended) <http://www.japaneselawtranslation.go.jp/law/detail/?id=2781&vm=04&re=02> [Accessed on July 19, 2021].
3. U.S. Department of Health and Human Services: 45 C.F.R. Part 46, 2018 (last amended).
4. World Medical Association: Declaration of Helsinki - Ethical Principles for Medical Research Involving Human, 2013 (last amended) <https://www.wma.net/policies-post/wma-declaration-of-helsinki-ethical-principles-for-medical-research-involving-human-subjects/> [Accessed on July 19, 2021].
5. World Medical Association: Declaration of Taipei on Ethical Considerations regarding Health Databases and Biobanks, 2016 (last amended) <https://www.wma.net/policies-post/wma-declaration-of-taipei-on-ethical-considerations-regarding-health-databases-and-biobanks/> [Accessed on July 19, 2021].
6. Khan I, Alwarsh M, Khan JI: A Comprehension Approach for Formalizing Privacy Rules of HIPAA for Decision Support, 2013 12th International Conference on Machine Learning and Applications, pp. 390–395, 2013.
7. Khan I, Sher M, Khan JI, Saqlain SM, Ghani A, Naqvi HA, Ashraf MU: Conversion of legal text to a logical rules set from medical law using the medical relational model and the world rule model for a medical decision support system. Informatics. **3**, 2–13, 2016.
8. Torr D, Soltana G, Sabetzadeh M, Briand LC, Auffinger Y, Goes P: Using models to anable compliance checking against the GDPR: an experience report. 2019 ACM/IEEE 22nd International Conference on Model Driven Engineering Languages and Systems (MODELS), 2019.
9. Deng M, Wuyts K, Scandariato R, Preneel B, Joosen W: A privacy threat analysis framework: supporting the elicitation and fulfillment of privacy requirements. Require Eng. **16**, 3–32, 2011.
10. Oliver I: Privacy Engineering: A Data Flow and Ontological Approach. CreateSpace Independent Publishing Platform. 2014.
11. Dewitte P, Wuyts K, Sion L, Landuyt DV, Emanuilov I, Valcke P, Joosen W: A comparison of system description models for data protection by design. The 34th ACM/SIGAPP Symposium, pp. 1512–1515. 2019.
12. Sion L, Dewitte P, Landuyt DV, Wuyts K, Valcke P, Joosen W: DPMF: a modeling framework for data protection by design. Int J Concept Modeling. **15**(10), 1–53, 2020.
13. Organisation for Economic Co-operation and Development: Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, 2013 (last amended).
14. International Organization for Standardization: ISO/IEC 29100, 2011.
15. World Health Organization International Agency for Research on Cancer: Common Minimum Technical Standards and Protocols for Biobanks Dedicated to Cancer Research, 2017.
16. Council for International Organizations of Medical Science: International Ethical Guidelines for Health-related Research Involving Humans, 2016.
17. Global Alliance for Genomics and Health: Framework for Responsible Sharing of Genomic and Health-Related Data, 2014.
18. Japanese Ministry of Education, Culture, Sports Science and Technology, Ministry of Health Labor, and Welfare and Ministry of Economy, Trade and Industry: Ethical Guidelines for Life Science, Medical and Health Research, 2021 <https://www.mhlw.go.jp/content/000757566.pdf> [Accessed on July 19, 2021] in Japanese.
19. U.S. Department of Health and Human Services: 45 CFR Parts 164, 2020.
20. European Commission Director-General for Health and Food Safety: Question and Answers on the interplay between the Clinical Trials Regulation and the General Data Protection Regulation, 2019.

Yuki KURODA

Yuki KURODA is currently a Ph.D. student at the Department of Social Informatics, Graduate school of Informatics, Kyoto University, Japan. He received his M.A. and J.D. from Osaka University and his LL.M. from the University of California, Berkeley. Besides conducting research, he practices law at Oh-Ebashi LPC & Partners (admitted in Japan and the State of New York). His current research interest includes medical informatics and regulatory issues on medical information processing.

Goshiro YAMAMOTO

Goshiro YAMAMOTO received his B.E., M.E., and Ph.D. in engineering from Osaka University. He is currently an associate professor in Kyoto University Hospital after being an assistant professor in Okayama University and Nara Institute of Science and Technology. His major research interest is human-computer interaction, digital transformation, and medical informatics.

Tomohiro KURODA

Tomohiro KURODA is the CIO (the director of division of medical information technology and administration planning) of Kyoto University Hospital, and the professor of medical informatics in graduate school of medicine and graduate school of informatics of Kyoto University. Besides serving as IT manager of healthcare organization for a decade, he has been a researcher of applied informatics, especially mixed reality and ubiquitous computing applications for medicine and welfare, since he received Ph.D. in information science from Nara institute of science and technology (NAIST), Japan in 1998.