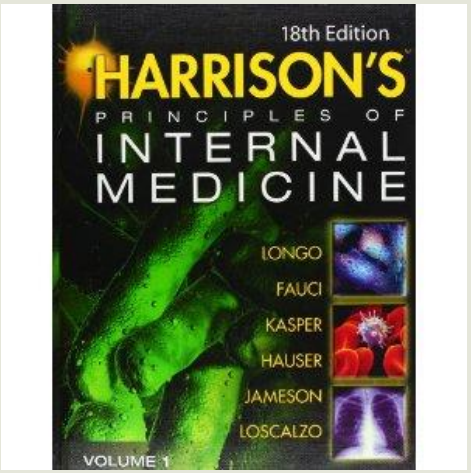
ELSI aspects of Health Database

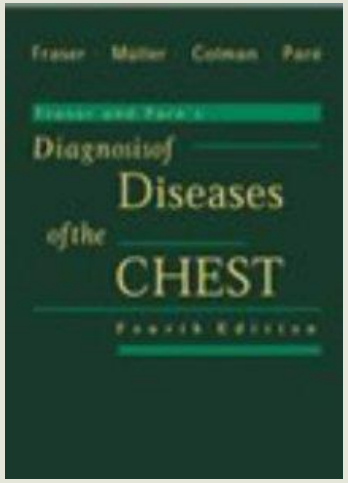
- ELSI: Ethical, Legal and social implications -

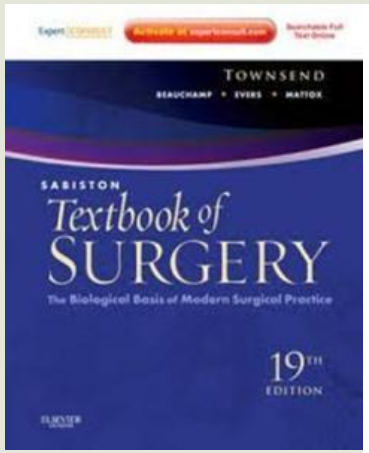
2022 Japan Interchange CDISC virtual Conference

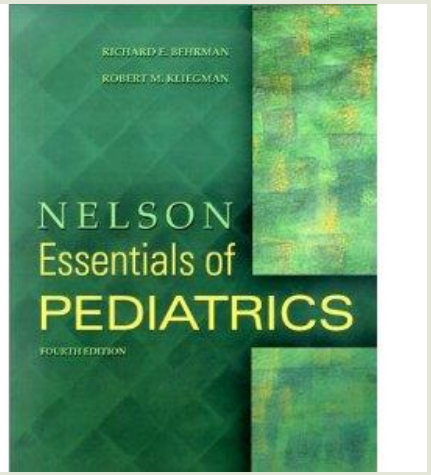
Ryuichi Yamamoto MD, PhD, Medical Information System Development Center
Tokyo, Japan

Medical knowledge is the accumulation of facts derived from past cases, refined from a myriad of privacy-sensitive information.









Public benefits and human right protection in Healthcare and Medical science field

- Ethics
  - Hippocratic oath
  - Nightingale Pledge
  - Declaration of Helsinki (WMA)
  - Declaration of Taipei on Ethical Considerations Regarding Health Databases And Biobank (WMA)
  - Nuremberg Code
- Legal
  - Penal Codes (JP)
    - Article 134 (Unlawful Disclosure of Confidential Information) physician, pharmacist, pharmaceuticals distributor, midwife, ・・・・
    - Other Nationally licensed professions have same legislation in determination Acts
  - Act on the Protection of Personal Information (2007 -)
  - Clinical Trial Act (2017 -)
- Legal Guidelines
  - Ethical Guidelines for Medical and Biological Research Involving Human Subjects
- Mass communication, Social Network System

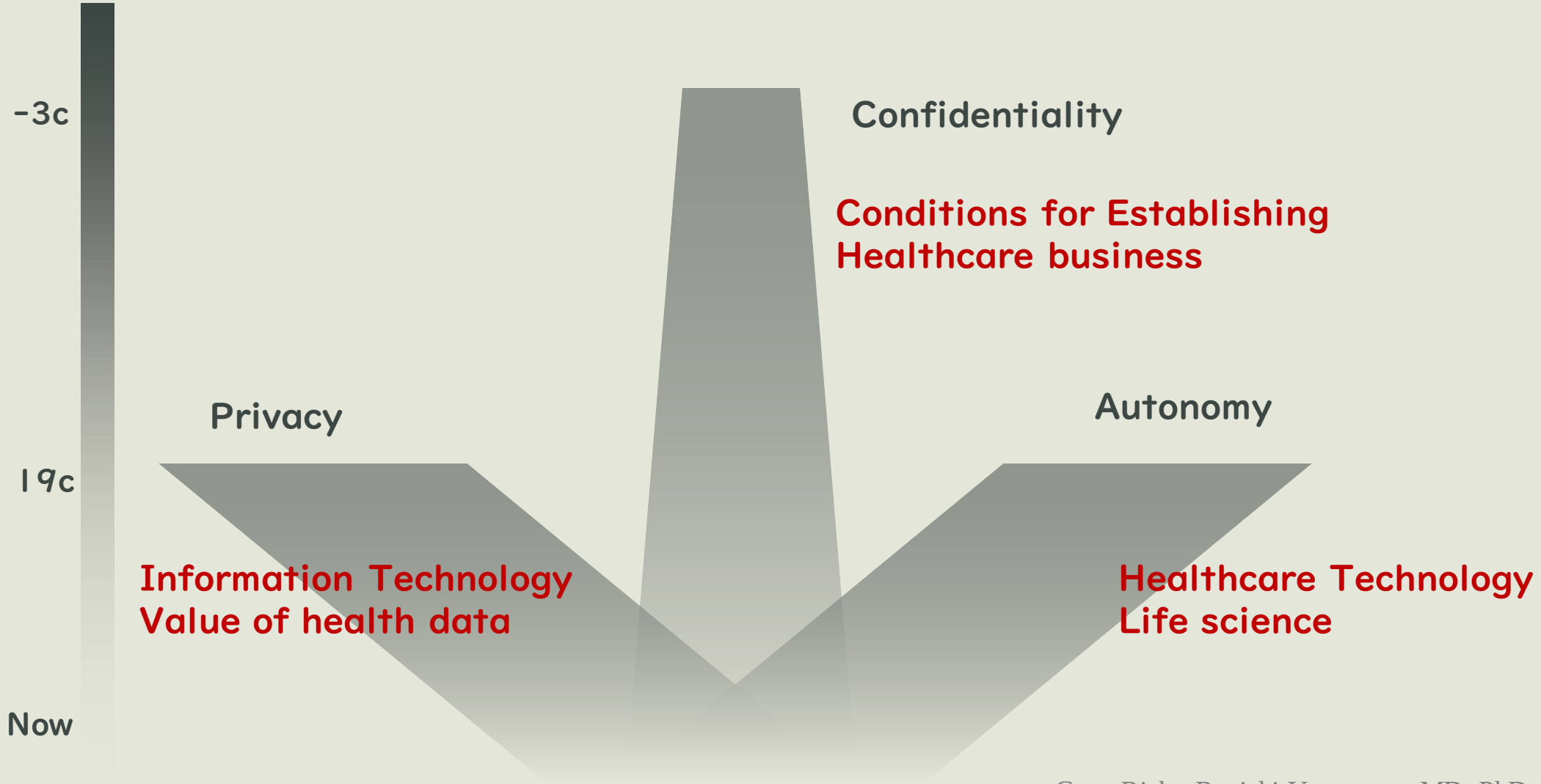
Ethical implications

Legal implications

Social implications

ELSI

Confidentiality and Human Rights in Healthcare Field



Should personal health data be used only for the patients themselves?

- **Only the individual has the right to control his or her own personal data.**
  - If the information has no public value, there is no problem as per the principle. Principles should be upheld to prevent a situation like the Nazi holocaust.
- **Can the person have a monopoly on the value of his or her information?**
  - In the medical field, personal information must be used to support medical care, advance medicine, and make social security sustainable.
  - Big data analysis is inevitable in personalized medicine and precision medicine.
- **Can we use patient's personal medical information without permission?**
  - Inadvertent information leaks lead to discrimination.
  - Medical institutions that use information in ways that patients do not agree with are shunned by patients.
- **Are privacy and public interest use in conflict?**

Act on the Protection of Personal Information (APPI) 2005 in Japan

- Specifying a Utilization Purpose and Restriction due to a Utilization Purpose
- Notification of a Utilization Purpose when Acquiring
- Proper Acquisition and Assurance about the Accuracy of Data Contents
- Security Control Action and Supervision over Employees and a Trustee
- Restriction on Third Party Provision
- Public Disclosure on Matters relating to Retained Personal Data
- Disclosure
- Correction and Utilization Cease

This Act covers personally identifiable information about the living

Issues of APPI 2005

- Protection was being pursued, but little was being done to address the lack of utilization.
  - How can it be used for public benefit without inconveniencing the person in question?
- Personal data protection legislation operates under different rules depending on the entity acquiring the information. (e.g. Private sector and Local Government sector)
  - Different definitions and regulations are a problem, but the more serious issue is that the responsible entities are different. (2000 rules problem)
- The definition of personal information was vague, i.e., anonymization could not be defined.
- There were no effective penalties for abuse.
- Obstacles to international transfer of personal information due to basic differences in legal systems from overseas.

Issues of APPI 2005

- Bias toward protection
- 2000 rules problem
- Vague definition of personal information
- No effective penalties for abuse
- Differences in legal systems from overseas

APPI 2017

- Bias toward protection
- 2000 rules problem
- Vague definition of personal information
  - The concepts of “individual identification code” and “anonymously processed information”
  - The concept of “Special care-required personal information”
- No effective penalties for abuse
  - Tighter penalties
  - Restriction of third-party provision with opt-out consent, and obligation of notification to the PPC
  - Obligation to prepare records pertaining to provision to a third party
  - Obligation to make efforts to erase personal data when necessary
- Differences in legal systems from overseas
  - Establishing Personal Information protection committee (PPC)
  - Clarification of the right to request disclosure, etc.

} Private sector only improve consistency with foreign countries.

Changes in APPI 2017

- Adding the concepts of “individual identification code” and “anonymously processed information”
- Adding The concept of “Special care-required personal information”
- Obligation to prepare records pertaining to provision to a third party
- Restriction of third-party provision with opt-out consent, and obligation of notification to the PPC
- Obligation to make efforts to erase personal data when necessary
- Clarification of the right to request disclosure, etc.
- Tighter penalties
- Establishing Personal Information protection committee (PPC)

Special care-required personal information

- race, creed, social status, medical history, criminal record, fact of having suffered damage by a crime, or other descriptions etc. prescribed by cabinet order as those of which the handling requires special care so as not to cause unfair discrimination, prejudice or other disadvantages to the principal.
- Special care-required personal information in cabinet order
  - (a) All medical information
  - (b) All health checkup information
  - (c) Crime related information
  - (d) Delinquency related information
- Shall not acquire special care-required personal information without obtaining in advance a principal's consent.
- A personal information handling business operator shall not provide special care-required personal information to a third party only with opt-out consent.

Impact of APPI 2017 on the use of health information

- Personal medical information can no longer be provided to third parties with opt-out consent. This prevents the flow of information to unexpected places. Also puts a stop to the easy gene business, etc.
- If anonymously processing can be done, health information can be provided to third parties for secondary use without consent, but for complex medical information, anonymously processing is not easy.
- Furthermore, anonymously processing makes it impossible to collate names, making it impossible to match information from multiple medical institutions.
- It is difficult to clarify the purpose and obtain explicit consent at the time of information collection in a backward-looking study using a database.

- Negative impact on the development of medical research, drug discovery, medical device development, and healthcare related industries is expected.
- After confirming the public interest in a broad sense, it is necessary to have a system that enables the utilization of anonymous processed information on the premise that it does not cause any disadvantage to patients and healthcare professionals.
- There needs to be a mechanism for collecting health information through opt-out consent while providing adequate opportunity for withdrawal of consent.

Next-Generation Medical Infrastructure Law (NGMIL) 2018

- Bias toward protection
  - The Next-Generation Medical Infrastructure Law (2018)
- 2000 rules problem

- Vague definition of personal information
  - The concepts of “individual identification code” and “anonymously processing information”
  - The concept of “Special care-required personal information”
- No effective penalties for abuse
  - Tighter penalties
  - Restriction of third-party provision with opt-out consent, and obligation of notification to the PPC
  - Obligation to prepare records pertaining to provision to a third party
  - Obligation to make efforts to erase personal data when necessary
- Differences in legal systems from overseas
  - Establishing Personal Information protection committee (PPC)
  - Clarification of the right to request disclosure, etc.

} Private sector only improve consistency with foreign countries.

The Act for Anonymized Health Information for Medical Research and Development (2018)

Known as: The Next-Generation Medical Infrastructure Law (NGMIL)

Aim:

- Regulations will be developed for businesses that anonymously processed medical information so that specific individuals cannot be identified, and through the secure and appropriate use of **anonymously processed medical information**, advanced research and development and the creation of new industries related to health and medicine will be promoted, thereby contributing to developing a **society of health and longevity**.

With Opt-out consent

PHR

Medical and health care institutes

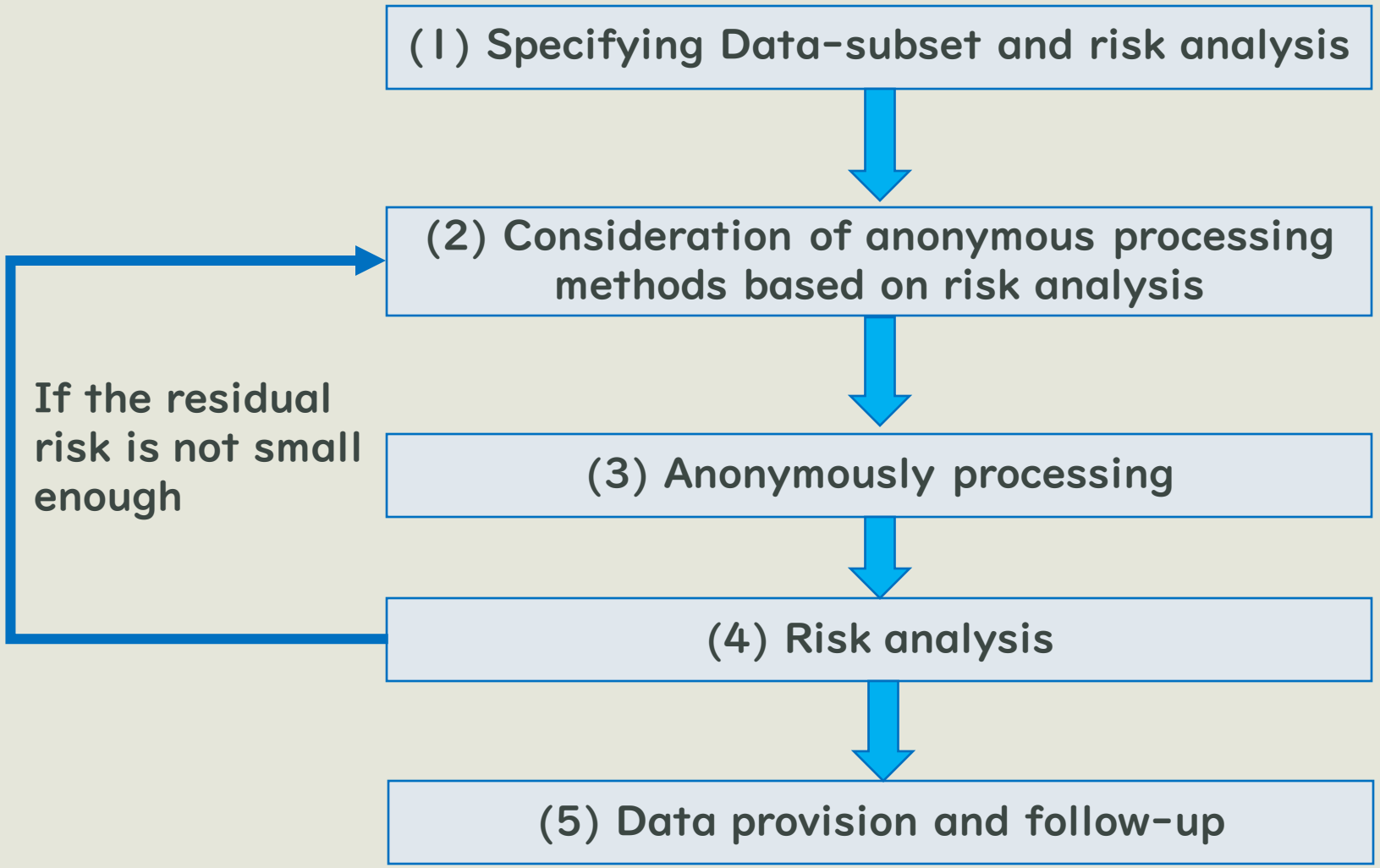
Personal health information

Authorized Anonymizing Health Data Organization

Anonymously processed medical information

Anonymously processed medical information users

Anonymously process in NGMIL



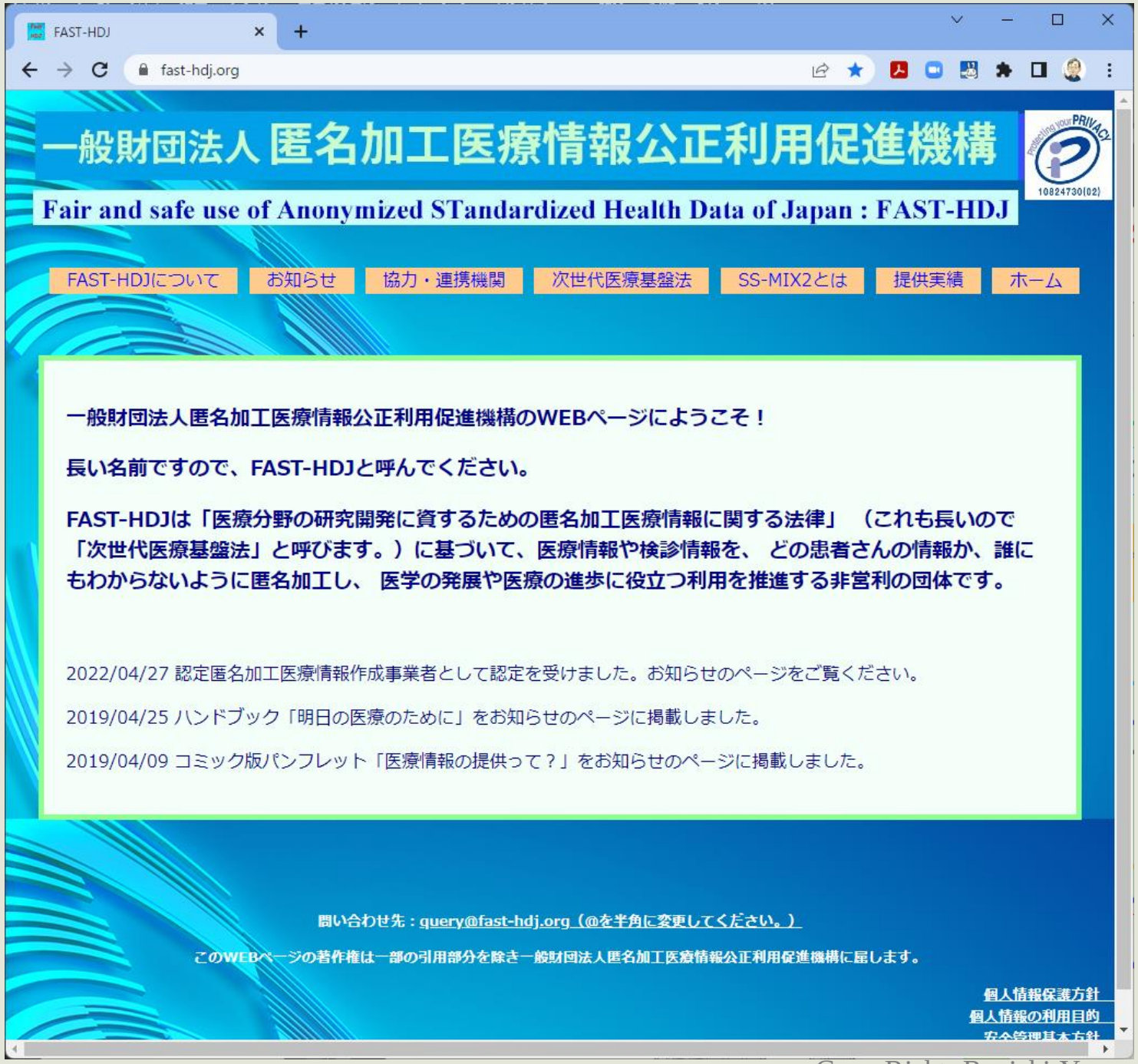
Deleting or random replacement of identifier

k-Anonymization of semi-identifier (K >= 3)

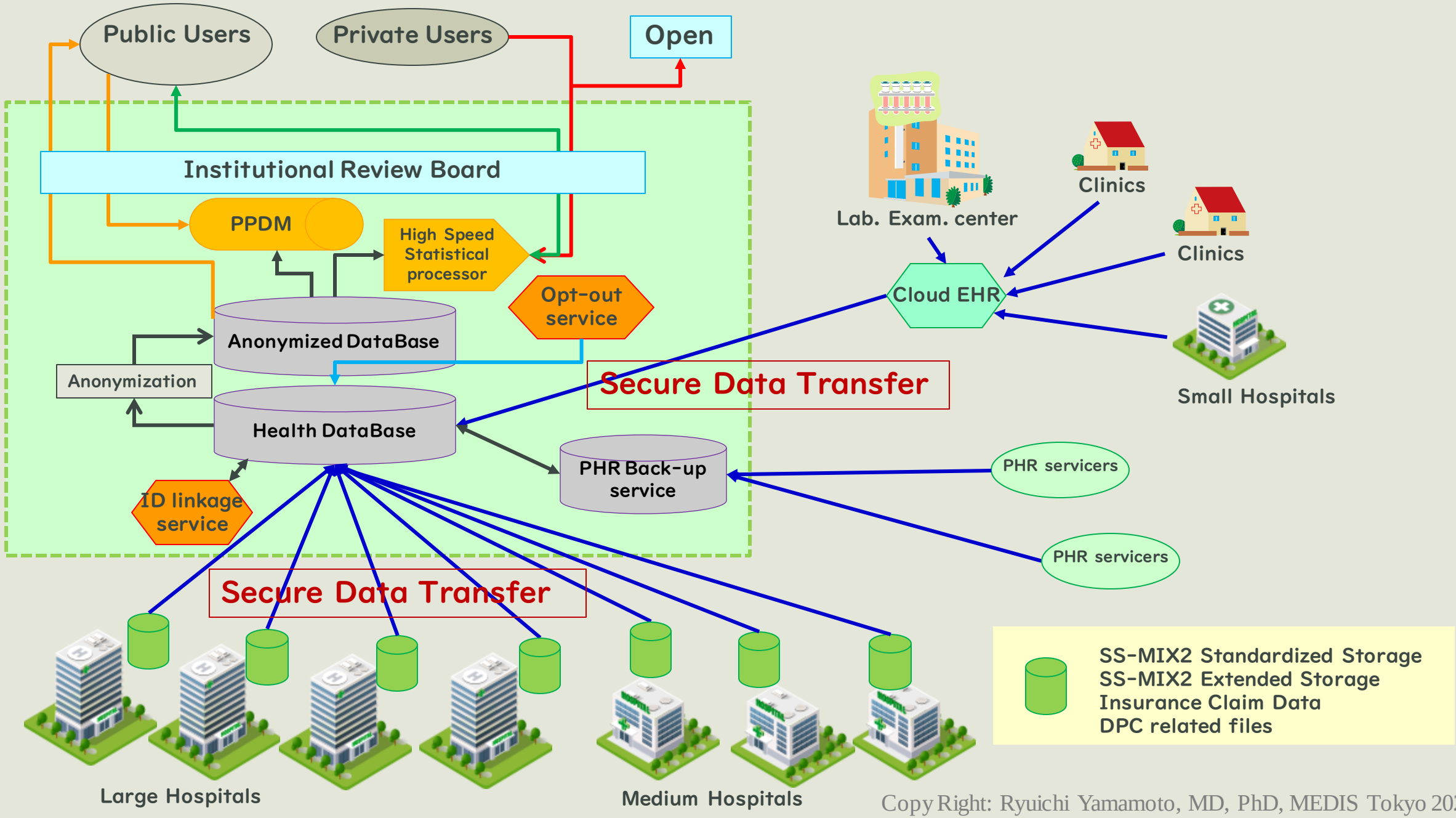
Generalization /Categorization

Top /Bottom coding

Micro-aggregation



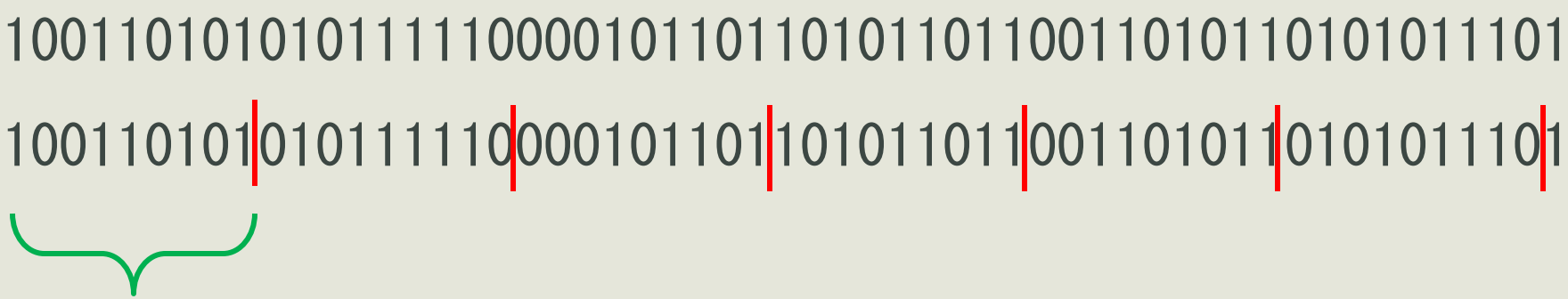
Fair and safe use of Anonymized Standardized Health Data of Japan (FAST-HDJ)



Issues of NGMIL

- Anonymization do not provide the perfect security
- Is opt-out consent effective?
- Should we consider other methods for secure analysis than anonymization?
- In the case of clinical research, the data must be linked to individual medical record information, if necessary, which is not possible with anonymized information.

Secure computing using secret sharing

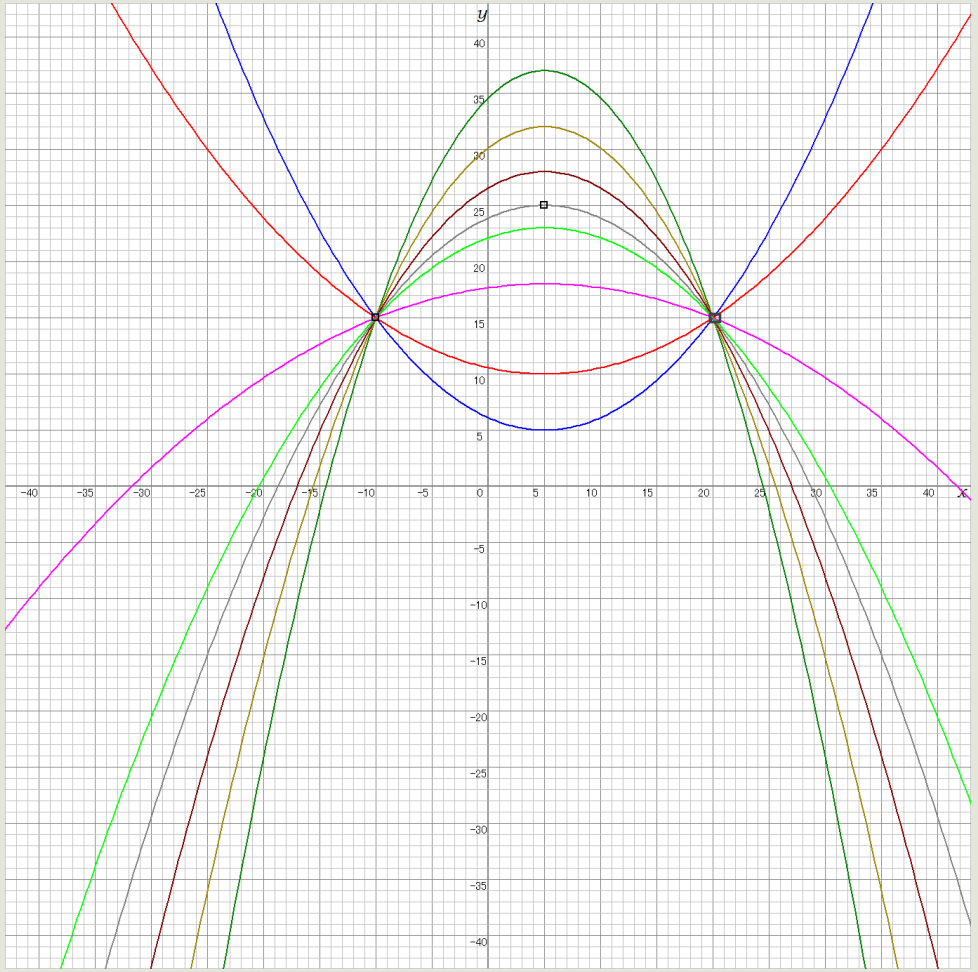


$2^q = 0 \sim 511 \quad \rightarrow \quad 100 \sim 611$

For example, in quadratic function $y = ax^2 + bx + c$,

$yi = axi + bxi + c, \qquad (x_1,y_1), (x_2,y_2), (x_3,y_3)$

With one (x_i,y_i) value, solving (a,b,c) value absolutely impossible.
With two (x_i,y_i) value, solving (a,b,c) value also absolutely impossible.
With three (x_i,y_i) value, solving (a,b,c) value is very easy.



f(-10) = 15 , f(20) = 15

There are infinitely many quadratic functions satisfying two different points.

f(-10) = 15 , f(20) = 15, f(5) = 20

There is only one quadratic function that satisfies three different points.

Implementation and evaluation of an efficient secure computation system using 'R' for healthcare statistics

Koji Chida,[1] Gembu Morohashi,[1] Hitoshi Fuji,[1] Fumihiko Magata,[1] Akiko Fujimura,[1] Koki Hamada,[1] Dai Ikarashi,[1] Ryuichi Yamamoto[2]

[1]Secure Platform Laboratories, NTT Corporation, Tokyo, Japan
[2]Department of Health Management and Policy, Graduate School of Medicine, University of Tokyo, Tokyo, Japan

Correspondence to
Dr Koji Chida, Secure Platform Laboratories, NTT Corporation, 3-9-11 Midori-cho, Musashino, Tokyo 180-8585, Japan; chida.koji@lab.ntt.co.jp

Received 6 January 2014
Revised 3 April 2014
Accepted 7 April 2014
Published Online First 24 April 2014

ABSTRACT

Background and objective While the secondary use of medical data has gained attention, its adoption has been constrained due to protection of patient privacy. Making medical data secure by de-identification can be problematic, especially when the data concerns rare diseases. We require rigorous security management measures.

Materials and methods Using *secure computation*, an approach from cryptography, our system can compute various statistics over encrypted medical records without decrypting them. An issue of secure computation is that the amount of processing time required is immense. We implemented a system that securely computes healthcare statistics from the statistical computing software 'R' by effectively combining secret-sharing-based secure computation with original computation.

Results Testing confirmed that our system could correctly complete computation of average and unbiased

stored in the database may be accessed inappropriately. If a data leak occurs, there is the risk of harm to the patients' privacy.

Security control measures for externally accessing databases include access controls and database encryption. Information identifying individual patients is not necessary for the purpose of statistical analysis. Therefore an effective method for protecting patient privacy is to store de-identified medical records in databases. However, risks and threats still remain, including inappropriate internal control, operational errors by administrators, as well as external attacks. Also, because in general encrypted data must be decrypted for use, the aforementioned risks and threats are still not completely eradicated. Furthermore, when it comes to de-identified data, the more unique the medical data, the easier it is to surmise the identity of the patient to whom the medical record belongs.

J Am Med Inform Assoc 2014;21:e326-e331. doi:10.1136/amiajnl-2014-002631

APPI 2020

- Bias toward protection
  - The Next-Generation Medical Infrastructure Law (2018)
  - The concepts of “pseudonymously processed information”
- 2000 rules problem

- Vague definition of personal information
  - The concepts of “individual identification code” and “anonymized personal data”
  - The concept of “Special care-required personal information”
- No effective penalties for abuse
  - More tighter penalties
  - Restriction of third-party provision with opt-out consent, and obligation of notification to the PPC
  - Obligation to prepare records pertaining to provision to a third party
  - Obligation to make efforts to erase personal data when necessary
- Differences in legal systems from overseas
  - Establishing Personal Information protection committee (PPC)
  - Clarification of the right to request disclosure, etc.

} Private sector only improve consistency with foreign countries.

Personal Information, Anonymously processed information, Pseudonymously processed information

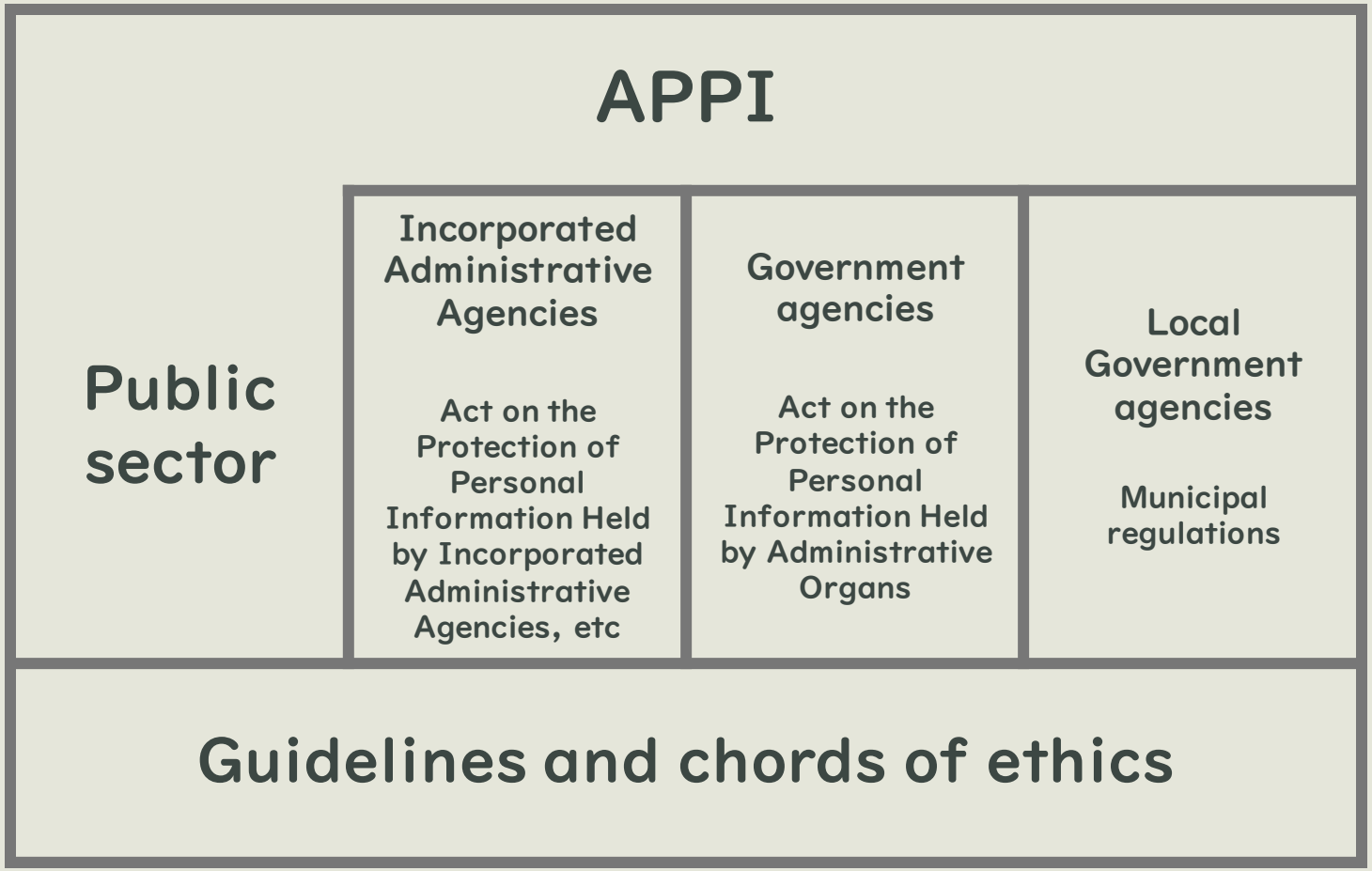
- Personal Information
  - Can be provided to a third party with consent.
  - Special care-required personal information cannot be to a third party with only opt-out consent.
- Pseudonymously processed information
  (Information on individuals obtained by processing personal information in such a way that specific individuals cannot be identified unless it is cross-checked with other information)
  - Purpose of use is specified in advance as much as possible.
  - Provision to third parties is prohibited in principle.
- Anonymously processed information
  - Can be provided to third parties without consent if re-identification is prohibited and efforts are made to ensure security management.

APPI 2021

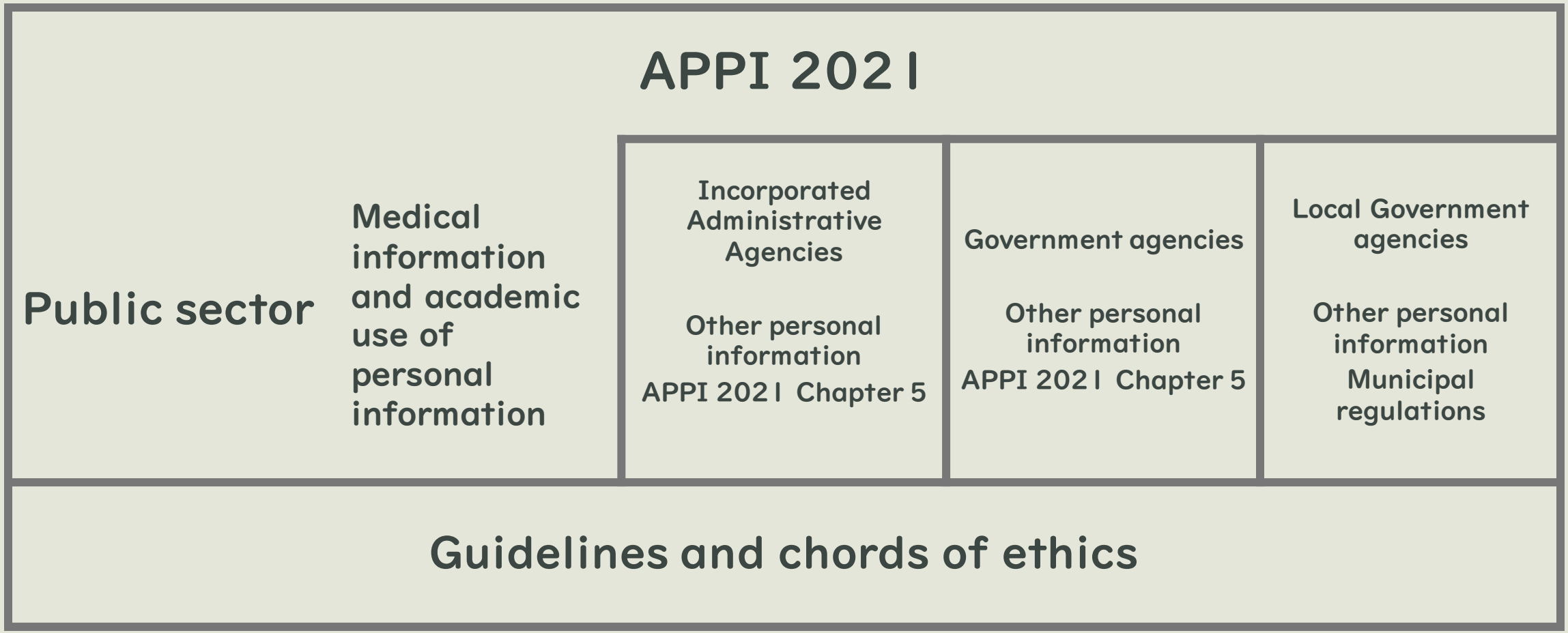
- Bias toward protection
  - The Next-Generation Medical Infrastructure Law (2018)
  - The concepts of “pseudonymously processed information
- 2000 rules problem
  - Integration of the handling of medical and academic information in government agencies, independent administrative agencies, and local government agencies.
- Vague definition of personal information
  - The concepts of “individual identification code” and “anonymized personal data”
  - The concept of “Special care-required personal information”
- No effective penalties for abuse
  - More tighter penalties
  - Restriction of third-party provision with opt-out consent, and obligation of notification to the PPC
  - Obligation to prepare records pertaining to provision to a third party
  - Obligation to make efforts to erase personal data when necessary
- Differences in legal systems from overseas
  - Establishing Personal Information protection committee (PPC)
  - Clarification of the right to request disclosure, etc.

} Private sector only improve consistency with foreign countries.

APPI 2005 - APPI 2020



APPI 2021



Academic use of health information APPI 2005 – 2020

- Article 76 (1) To a person set forth in each following item who is a personal information handling business operator shall the provisions of Chapter IV not apply when a whole or part of the purpose of handling personal information etc. is a purpose prescribed in each said item respectively.
  - (i) a broadcasting institution, newspaper publisher, communication agency and other press organization (including an individual engaged in the press as his or her business):a purpose of being provided for use in the press
  - (ii) a person who practices writing as a profession: a purpose of being provided for use in writing
  - (iii) a university and other organization or group aimed at academic studies, or a person belonging thereto: a purpose of being provided for use in academic studies
  - (iv) a religious body: a purpose of being provided for use in a religious activity (including those activities accessory thereto)
  - (v)a political body: a purpose of being provided for use in a political activity (including those activities accessory thereto)
- (2) ・・・
- (3) A personal information handling business operator etc. set forth in each item of paragraph (1) shall strive to take itself necessary and appropriate action for the security control of personal data or anonymously processed information and necessary action to ensure the proper handling of personal information etc. such as dealing with a complaint about the handling of personal information etc., as well as announce to the public the contents of such action taken.

Chapter IV contains all the obligations of a business operator handling personal information.

Academic use of health information APPI 2021

- Article 57 (1) To a person set forth in each following item who is a personal information handling business operator shall the provisions of Chapter IV not apply when a whole or part of the purpose of handling personal information etc. is a purpose prescribed in each said item respectively.
  - (i) a broadcasting institution, newspaper publisher, communication agency and other press organization (including an individual engaged in the press as his or her business):a purpose of being provided for use in the press
  - (ii) a person who practices writing as a profession: a purpose of being provided for use in writing
  - (iii) a religious body: a purpose of being provided for use in a religious activity (including those activities accessory thereto)
  - (iv)a political body: a purpose of being provided for use in a political activity (including those activities accessory thereto)
- (2) ・・・
- (3) A personal information handling business operator etc. set forth in each item of paragraph (1) shall strive to take itself necessary and appropriate action for the security control of personal data or anonymously processed information and necessary action to ensure the proper handling of personal information etc. such as dealing with a complaint about the handling of personal information etc., as well as announce to the public the contents of such action taken.

Chapter IV contains all the obligations of a business operator handling personal information.

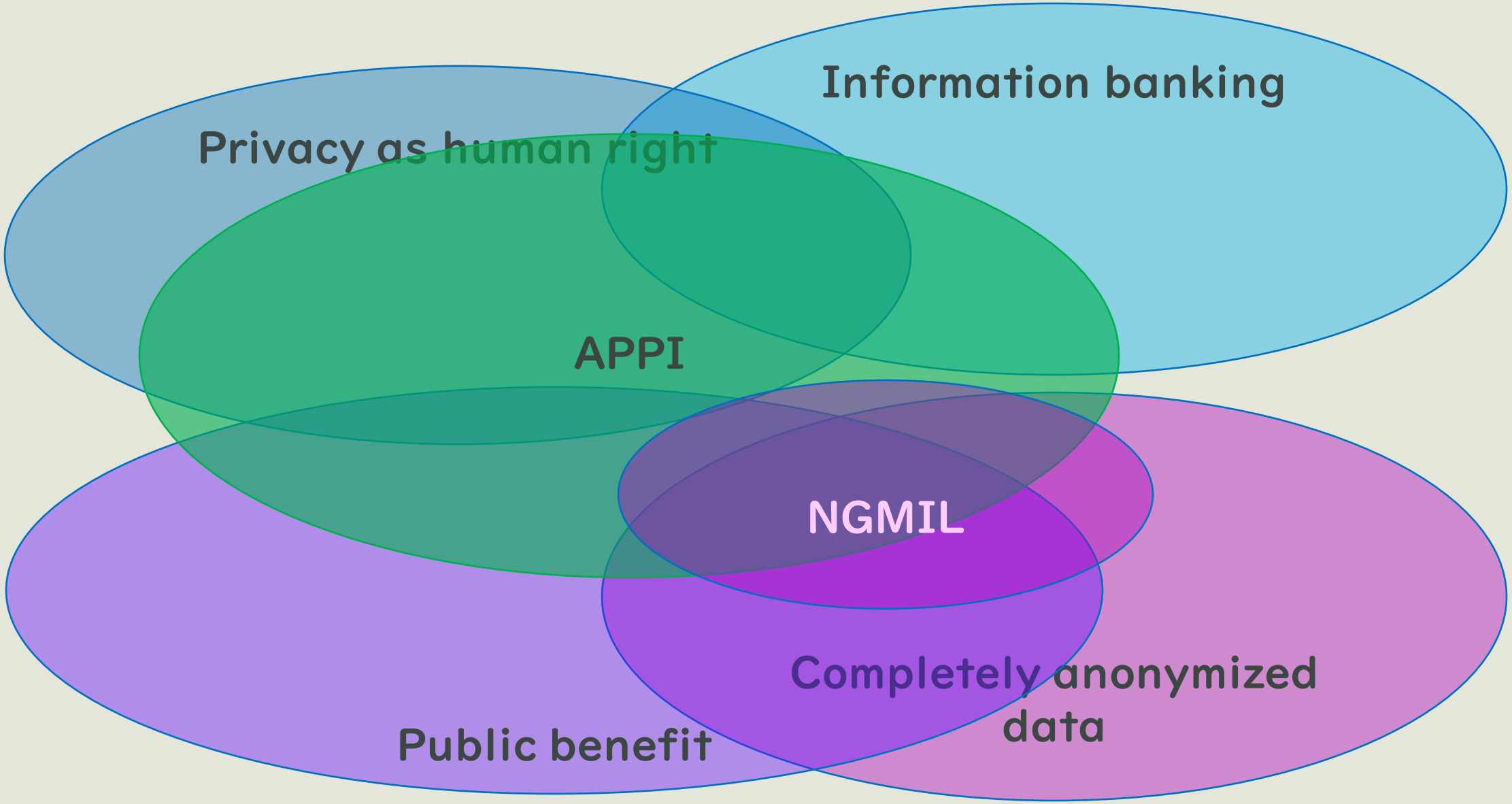
Academic use of health information APPI 2021

- Chapter IV Article 18 (Notification etc. of a Utilization Purpose when Acquiring)
- (1) A personal information handling business operator shall, in case of having acquired personal information except in cases where a utilization purpose has been disclosed in advance to the public, promptly inform a principal of, or disclose to the public, the utilization purpose.
- (2) (3) ・・・
- (4) The provisions of the preceding three paragraphs shall not apply in those cases set forth in the following.
  - i. cases in which there is a possibility that informing a principal of, or disclosing to the public, a utilization purpose would harm a principal or third party's life, body, fortune or other rights and interests
  - ii. cases in which there is a possibility that informing a principal of, or disclosing to the public, a utilization purpose would harm the rights or legitimate interests of the said personal information handling business operator
  - iii. cases in which there is a need to cooperate in regard to a central government organization or a local government performing affairs prescribed by laws and regulations, and when there is a possibility that informing a principal of, or disclosing to the public, a utilization purpose would interfere with the performance of the said affairs
  - iv. cases in which it can be recognized, judging from the acquisitional circumstances, that a utilization purpose is clear
  - v. When the Business Operator Handling Personal Information is an academic research institution, etc., and it is necessary to handle said Personal Information for the purpose of using it for academic research. This includes cases where a part of the purpose of handling said personal information is for academic research purposes and excludes cases where there is a risk of unjustified infringement on the rights and interests of individuals.
  - vi. When personal data is provided to an academic research institution, etc., and it is necessary for said academic research institution, etc. to handle said personal data for academic research purposes.

Similar provisions are found only in Articles 20 (Security Control Action) and 27 (Restriction on Third Party Provision of Personally Referable Information).

Ethical Guidelines for Medical and Biological Research Involving Human Subjects

- Epidemiology Ethical Guidelines (2002, 2007), Ethical Guidelines for Clinical Research (2003, 2008)
  Ethical Guidelines for Medical Research Involving Human Subjects (2014)
  - Anonymization with linking table??
- Ethical Guidelines for Medical Research Involving Human Subjects (2017)
  - Still concept of anonymization with linking table exist.
- Ethical Guidelines for Medical and Biological Research Involving Human Subjects (2021)
  - Integrate the Ethical Guidelines for Human Genome and Genetic Analysis Research into this guidelines.
  - Digital consent in Informed Consent
  - Still concept of anonymization with linking table exist.
- Ethical Guidelines for Medical and Biological Research Involving Human Subjects (2022)
  - Terminology is completely unified to APPI
    No anonymization with linking table
  - pseudonymously processed information is introduced



Selectable Branches in Observational Studies from the ELSI Perspective

- **Personal Information**
  - With proper consent, personal information can be directly utilized for observational research.
  - Is it possible to obtain re-consent with already accumulated information?
- **Pseudonymously Processed Information**
  - Not substantially different from utilizing personal information. Requires appropriate consent.
  - Security management is generally easier.
- **Anonymously Processed Information**
  - Observational studies can be conducted without consent if only data from one institute are used.
  - There are limitations to being an anonymous process. (Rare examples are difficult to handle. Names cannot be collated in anonymously processed form.)
- **Act on Anonymized Medical Data That Are Meant to Contribute to Research and Development in the Medical Field (NGMIL)**
  - From the perspective of the APPI, it falls under the "use stipulated by other laws and regulations" and only needs to comply with the NGMIL
  - Authorized Anonymizing Health Data Organization can create anonymized processed medical information after collation of the same person's information from multiple facilities.
  - No need to comply with "Ethical guidelines for life science and medical research involving human subjects".

Shared Use is permitted, but some limitations requiring careful attention

Thank you for your attention!