

Addressing Challenges in Cross-Border Medical and Health Data Exchange

寺本, 振透
Faculty of Law, Kyushu University : Professor

<https://hdl.handle.net/2324/7157009>

出版情報 : 2023-10-21
バージョン :
権利関係 :





KYUSHU UNIVERSITY

Addressing Challenges in Cross-Border Medical and Health Data Exchange

2023年第三届“数字法治与智慧司法”国际研讨会

October 21, 2023



Shinto TERAMOTO

Professor of Law, Kyushu University, Fukuoka, Japan

teramoto.shinto.717@m.kyushu-u.ac.jp

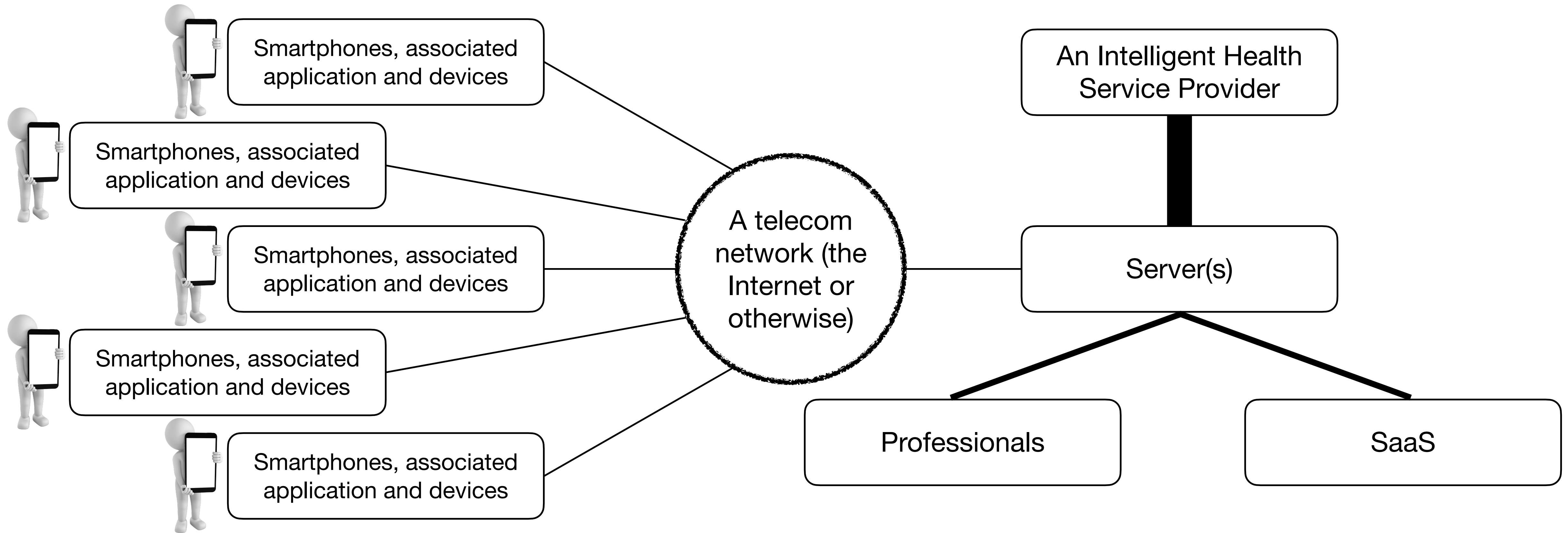
shin.teramoto@terrara.net

Use Cases for Intelligent Health

Use Cases for Intelligent Health

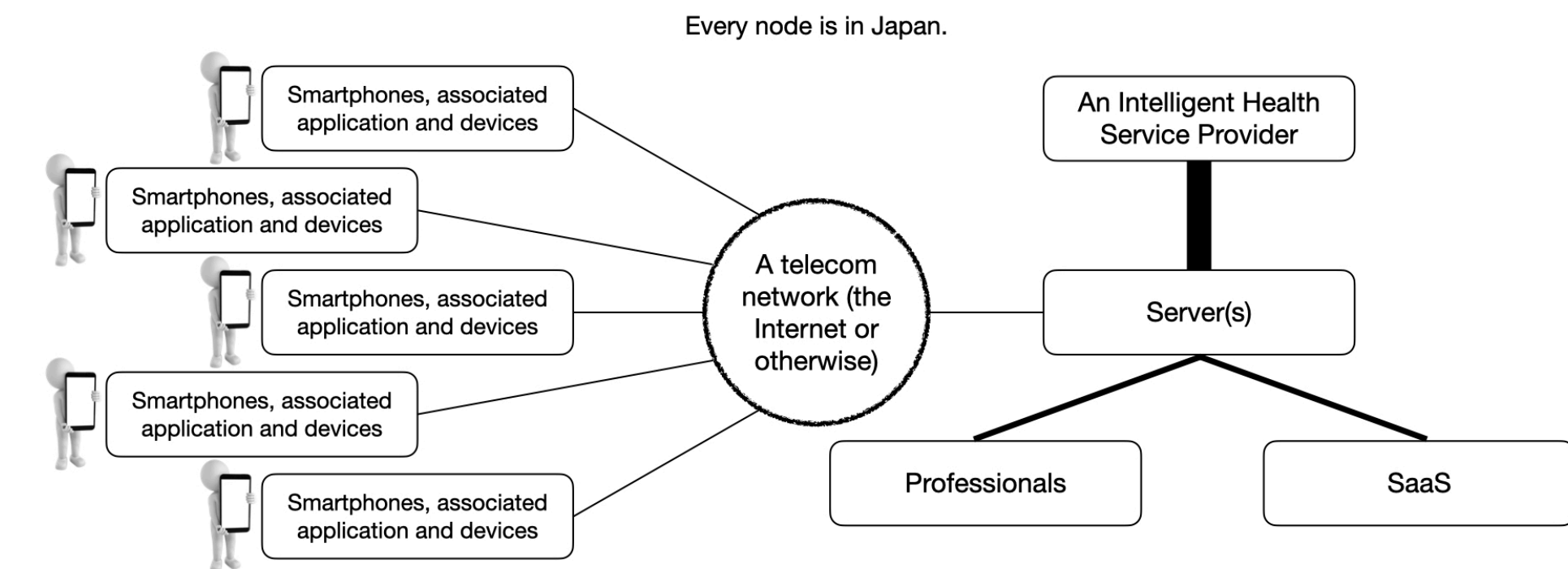
A Simple, But Not Very Realistic, Use Case

Every node is in Japan.



Use Cases for Intelligent Health

A Simple, But Not Very Realistic, Use Case

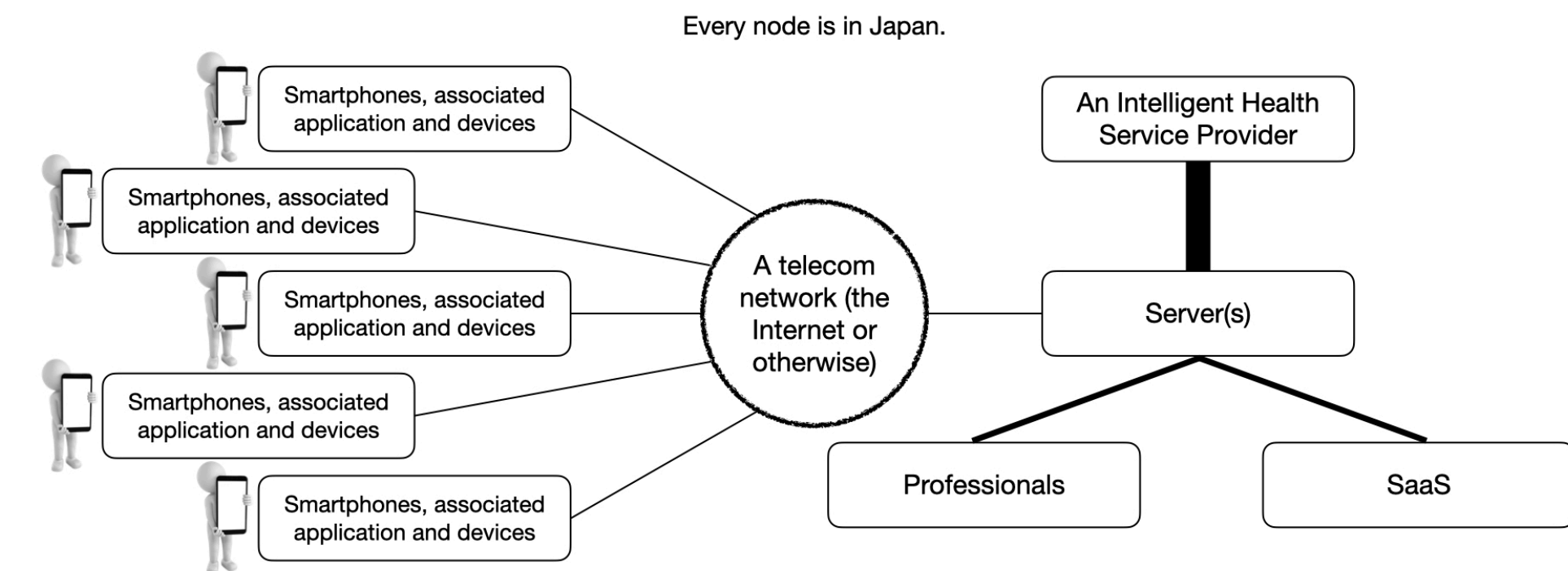


- In this use case, all nodes are located within a single jurisdiction.
- The scheme

- The Intelligent Health Service Provider is a Japanese company that provides services through offices and establishments located in Japan.
- The subscribers of the said service are Japanese nationals who are located in Japan when using the service, and naturally, the smartphones connecting them to the provider are also located in Japan.
- Personal health-related devices such as scales, blood pressure monitors, blood glucose meters, and heart rate monitors, and the servers handling the data derived from them, are located in Japan.
- Professionals and Software as a Service (SaaS) that provide supervision and services constituting a part of the said Intelligent Health Service operate within Japan.

Use Cases for Intelligent Health

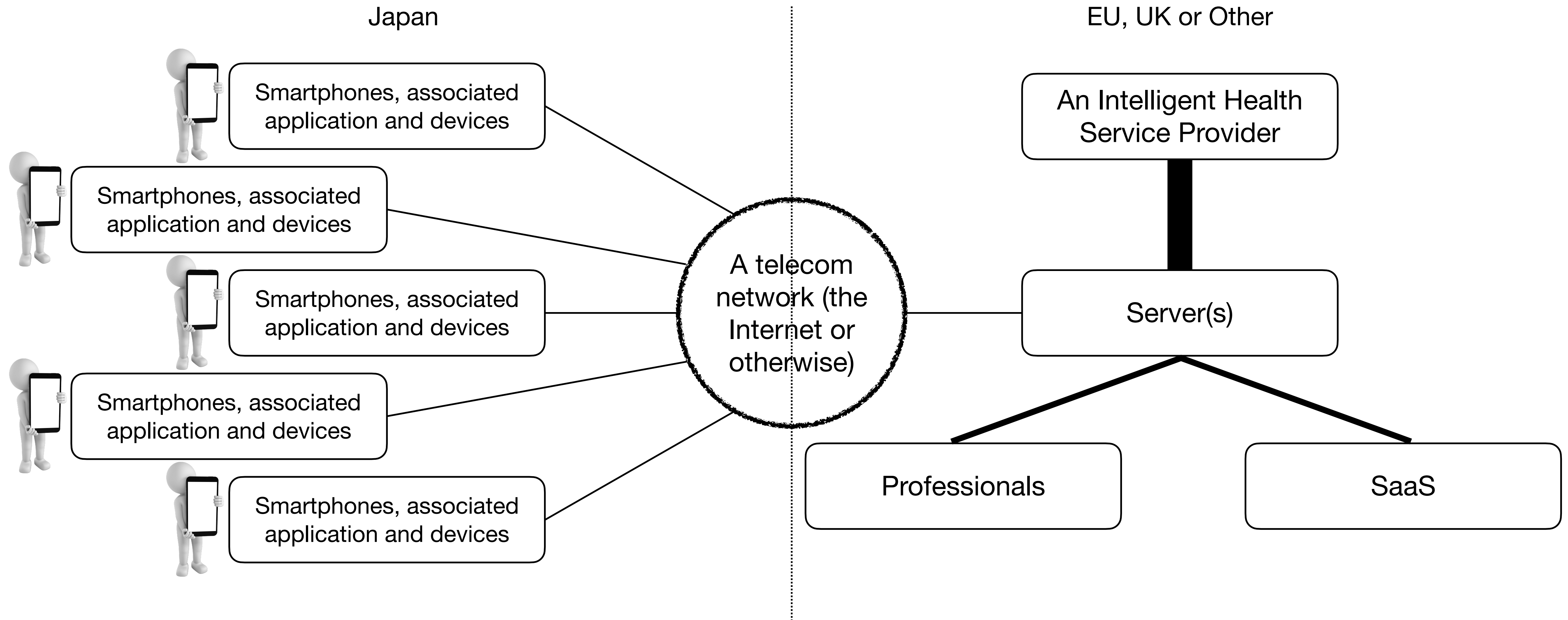
A Simple, But Not Very Realistic, Use Case



- Major procedures to protect personal information.
- Essentially, all issues are governed by the Act on the Protection of Personal Information (Act No. 57 of 2003; “APPI”), the Civil Code (Act No. 89 of 1896), and other relevant Japanese laws. Depending on the specific conditions, this may also include the Telecommunications Business Act (Act No. 86 of 1984).
- It's both essential and almost indisputable that the Service Provider must disclose to individual subscribers the purposes of using their medical and health data, as well as with which other businesses and for what purposes they will share this data, and then obtain the subscribers' consent. See, for example, Articles 17, 18, 21, 27 of APPI.

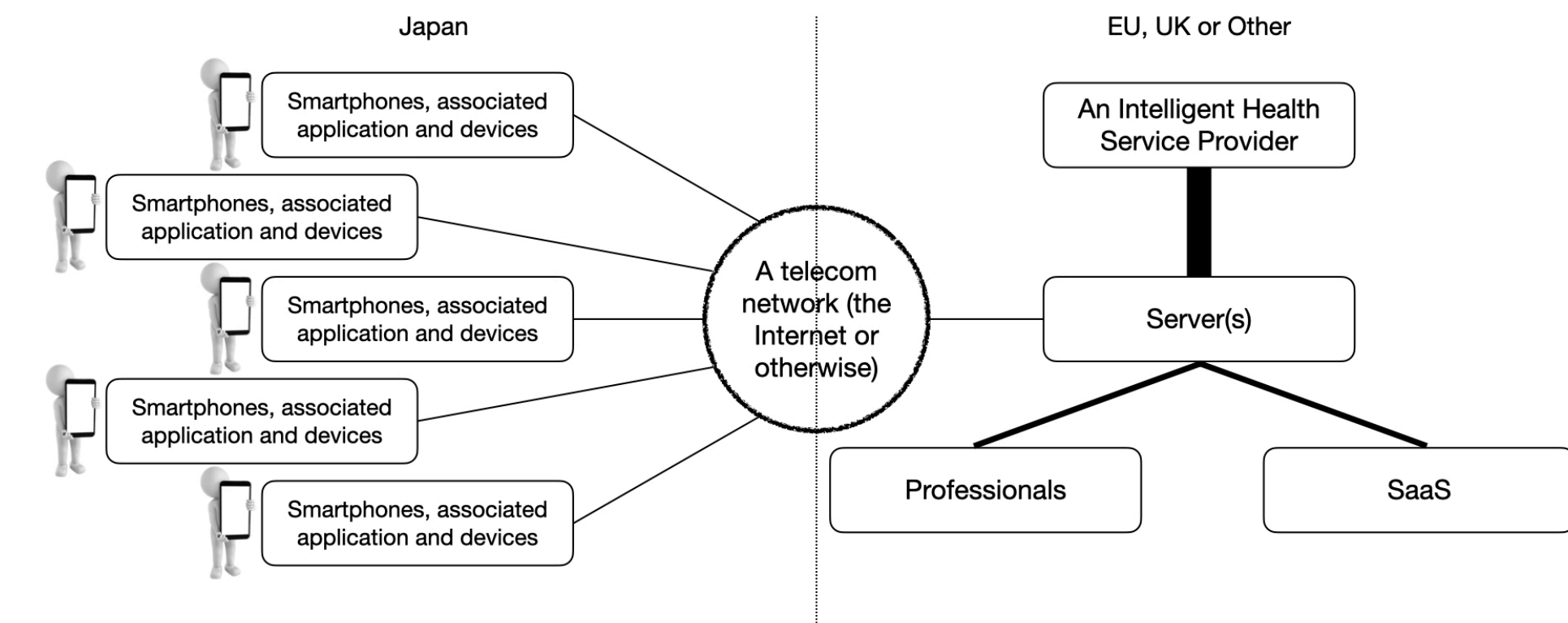
Use Cases for Intelligent Health

A Use Case Spanning At Least Two Jurisdictions



Use Cases for Intelligent Health

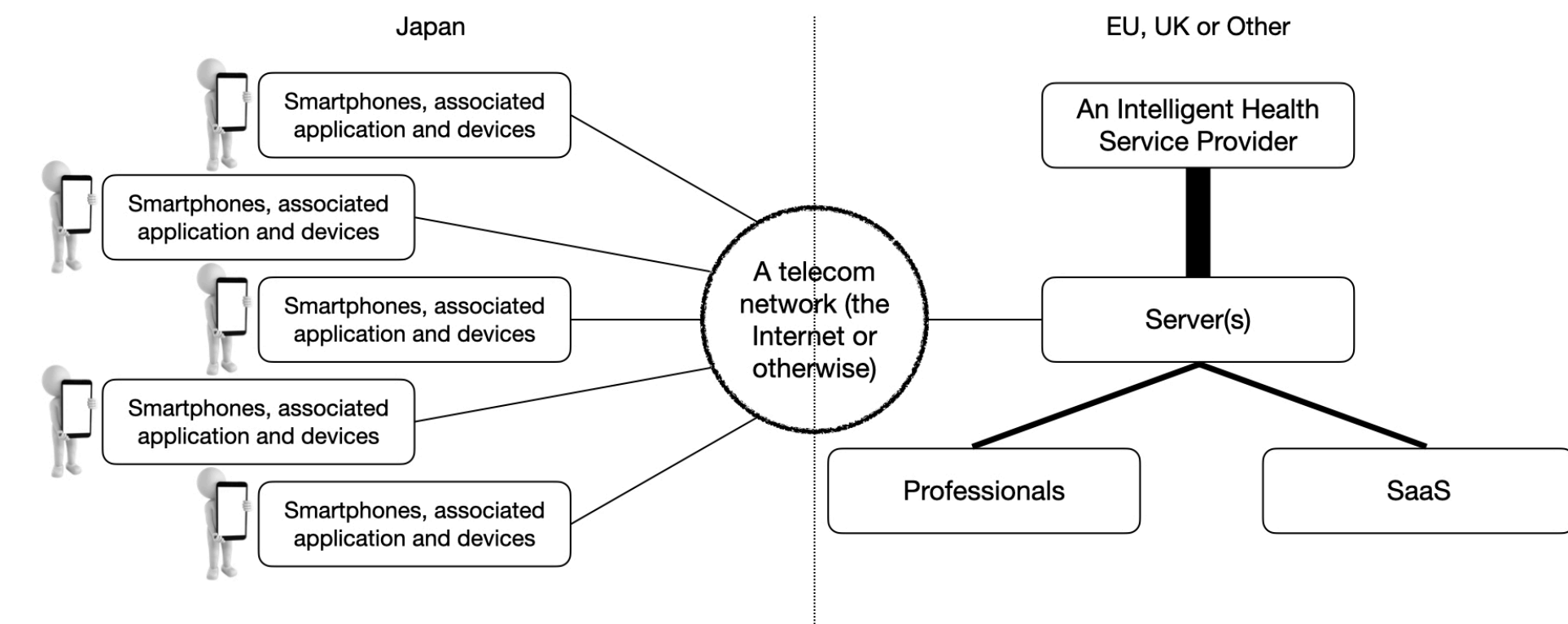
A Use Case Spanning At Least Two Jurisdictions



- Nodes are distributed among at least two jurisdictions.
- The scheme
 - The Intelligent Health Service Provider is a foreign company that provides services through offices and establishments located in a specific foreign country.
 - The subscribers of the said service are Japanese nationals who are located in Japan when using the service, and naturally, the smartphones connecting them to the provider are also located in Japan.
 - Personal health-related devices such as scales, blood pressure monitors, blood glucose meters, and heart rate monitors, and the servers handling the data derived from them, are located in Japan.
 - Collaborative professionals and SaaS operate within the same foreign country as the aforementioned Provider.

Use Cases for Intelligent Health

A Use Case Spanning At Least Two Jurisdictions



6

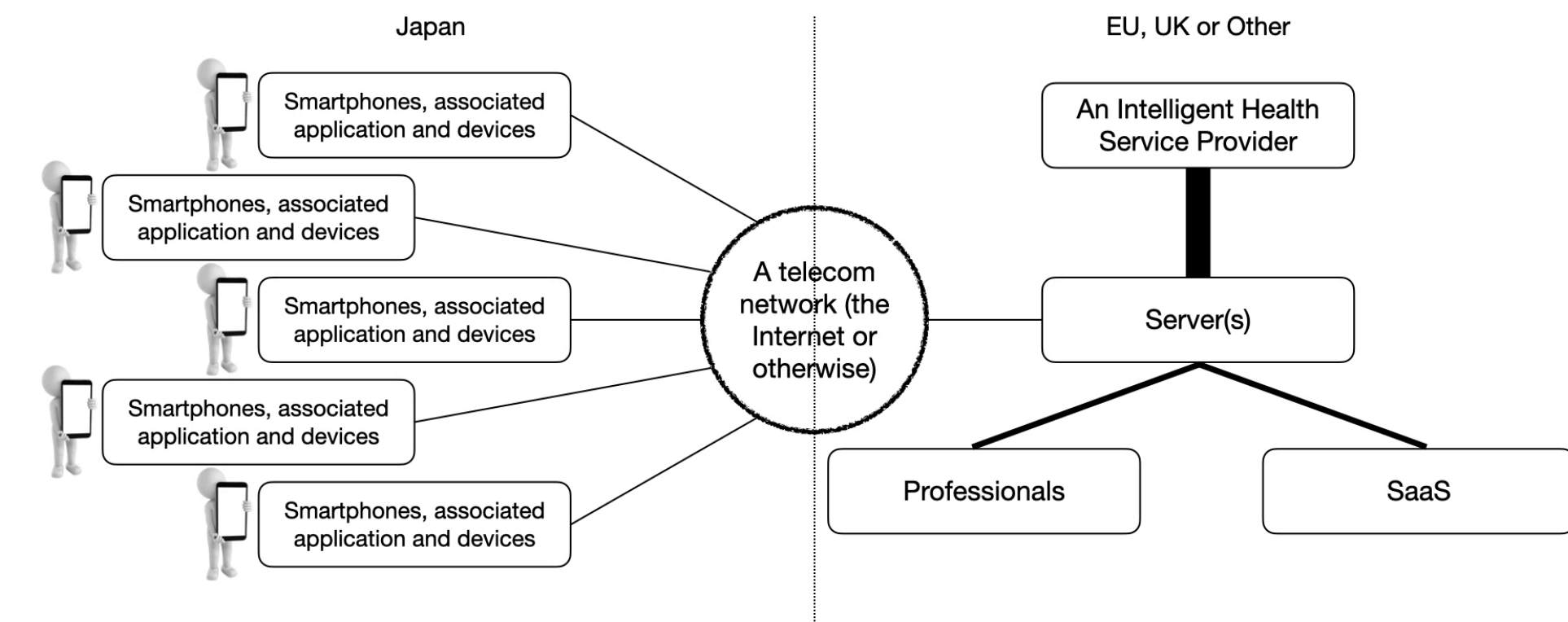
- The service provision by the Provider to Japanese subscribers is not accidental but rather intentionally carried out by the Provider itself. Therefore, there's no doubt that the Provider is subject to APPI.
- Furthermore, it's important to note that the medical and health data of subscribers are being shared with third parties located abroad. Sharing such information with third parties in countries where the level of personal information protection is not assured to be on par with Japan's standards is subject to stricter restrictions.

- Article 28, Para. 2 of the APPI requires the Service Provider to inform subscribers in advance about the “information on the personal information protection system of the foreign country, on the measures the third party takes for the protection of personal information, and other information that is to serve as a reference to that person, pursuant to Order of the Personal Information Protection Commission”.

- The Provider faces a significant challenge.
 - What should they disclose to subscribers in order to obtain valid informed consent for the acquisition, sharing, and use of their medical and health data?
- The information to be disclosed to the subscribers may include:
 - i) That the medical and health data of the subscribers will be transmitted to the jurisdiction in which the Provider operates;
 - ii) That the data will be shared with specific third parties in that jurisdiction, along with their individual levels of personal information protection; and
 - iii) The level of personal information protection legally available in that jurisdiction.
- It would be desirable to assume that the legal counsels, who assisted the Provider in their decision to offer services to Japanese subscribers, comprised a team including lawyers from both countries. They should have thoroughly gathered and examined information on the similarities and differences in personal information protection between the provider's jurisdiction and Japan for that purpose. However, the reality is that the desirable situation isn't always achieved.

Use Cases for Intelligent Health

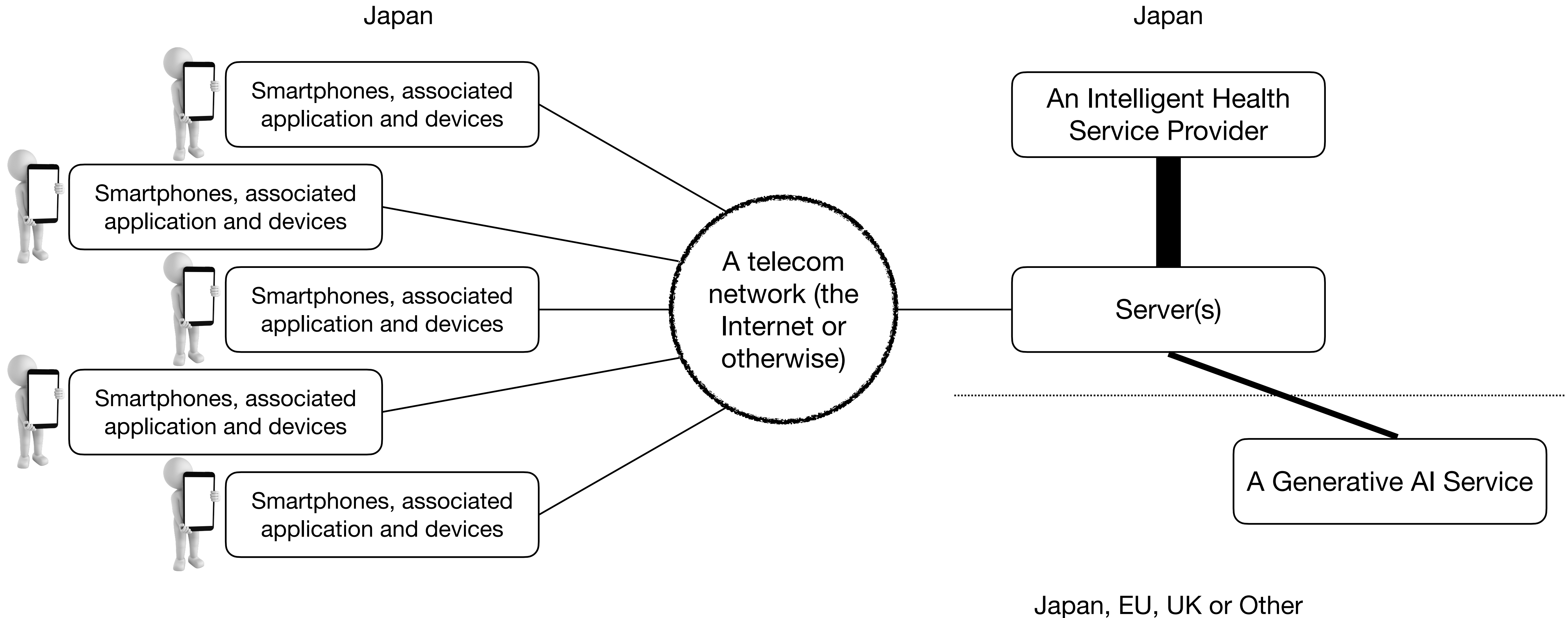
A Use Case Spanning At Least Two Jurisdictions



6

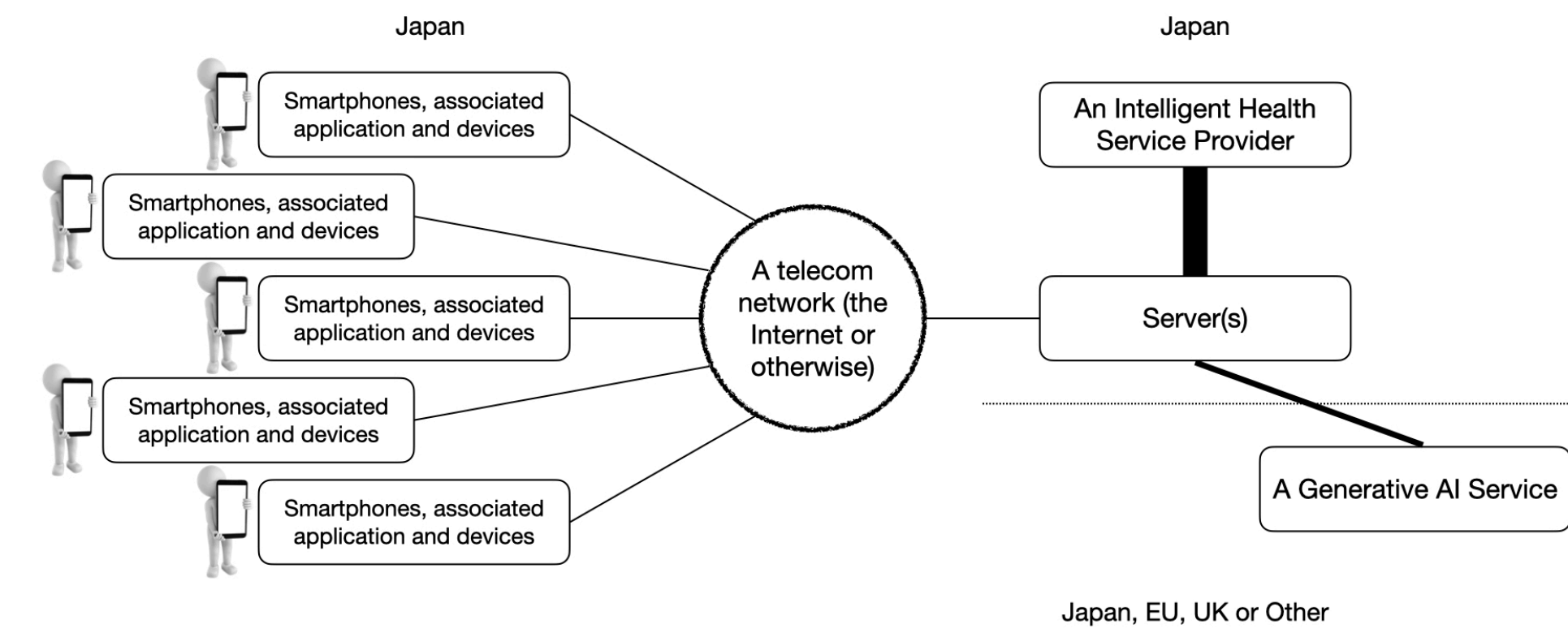
Use Cases for Intelligent Health

Another Use Case Involving a Generative AI Service



Use Cases for Intelligent Health

Another Use Case Involving a Generative AI Service

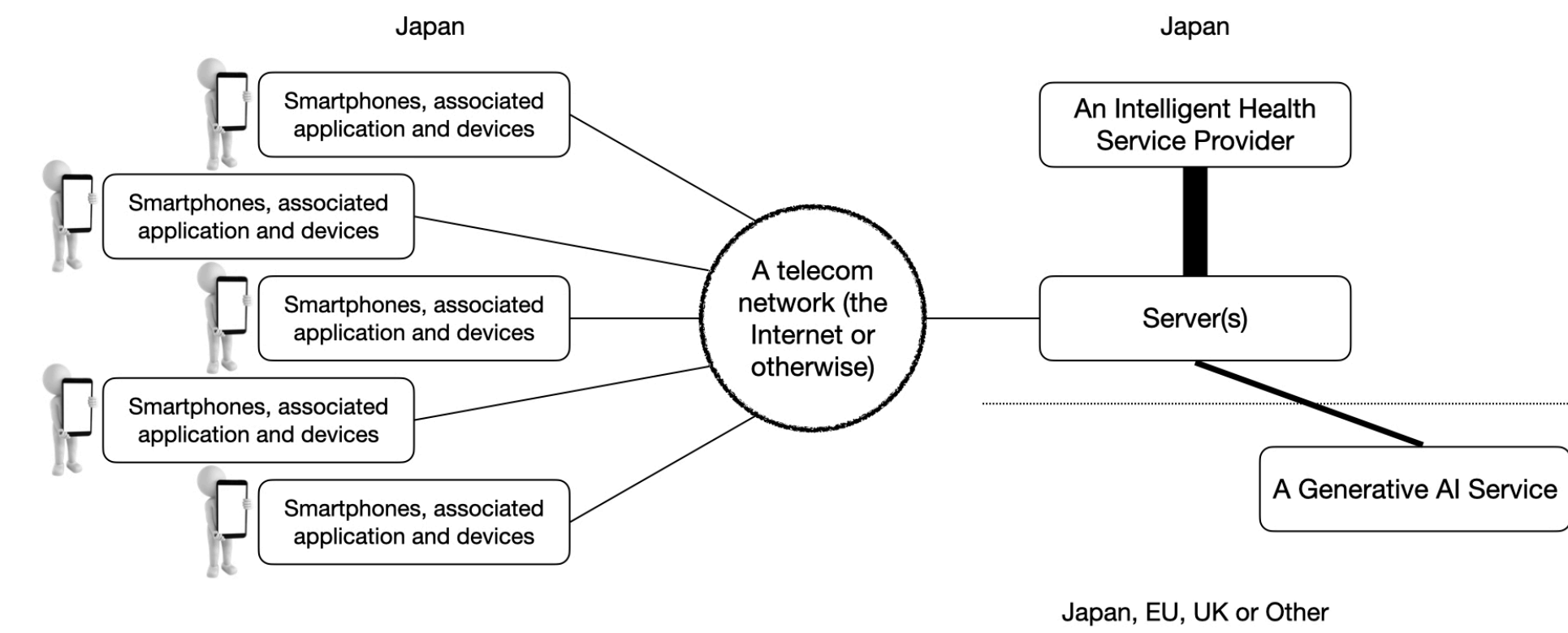


- The scheme

- The Intelligent Health Service Provider is a Japanese company that provides services through offices and establishments located in Japan.
- The subscribers of the said service are Japanese nationals who are located in Japan when using the service, and naturally, the smartphones connecting them to the provider are also located in Japan.
- Personal health-related devices such as scales, blood pressure monitors, blood glucose meters, and heart rate monitors, and the servers handling the data derived from them, are located in Japan.
- The Provider transmits data to a generative AI service provider to produce feedback in either or both text and image forms for individual subscribers.

Use Cases for Intelligent Health

Another Use Case Involving a Generative AI Service



10

• Challenges

- The level of personal information protection offered by the generative AI service provider is likely uncertain. Notably, the personal information of one subscriber might inadvertently be used to generate feedback for another subscriber.
- Physicians and legal counsels also draw upon their experiences from providing care or consultation to individual patients and clients. To date, the disclosure of personal information from former patients and clients to subsequent ones has perhaps been rare, likely because of their stringent adherence to professional ethics. Yet, we seem to have not found a way to integrate such adherence into the design of the generative AI system.
- If the generative AI service is provided from a foreign country, the issues identified in the aforementioned use case also apply.
- Using AI services increase concerns about the level of personal information protection.

Concerns About the Current Personal Data Protection Legislation

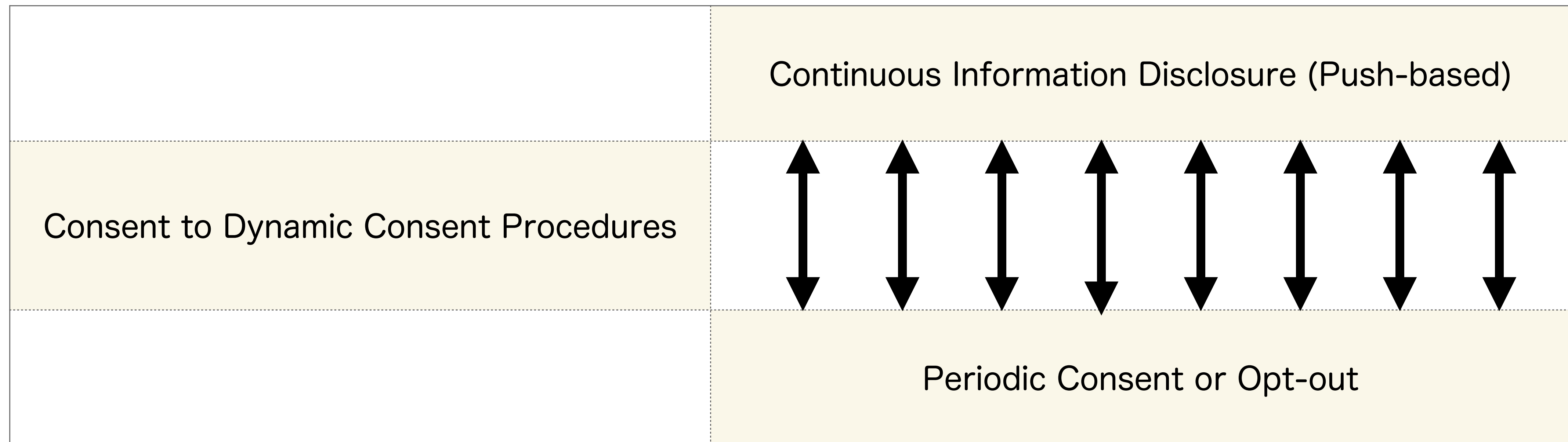
- It is not realistic to assemble all the technical or service components required to constitute an Intelligent Health Service that meets the standards satisfying subscribers within a single country. Therefore, the transmission and sharing of medical and health data across borders is inevitable.
- Legislation protecting personal information and their levels of protection vary across jurisdictions.
 - While some might believe that differences in protection among countries can be addressed by international agreements setting a minimum level of protection or by rules from international organizations, practitioners in the field of intellectual property know well that this is not the case.
 - Despite the presence of conventions such as the Berne Convention, the Paris Convention, and TRIPS, countries have either introduced new laws, adapted their existing ones, or confirmed their alignment with these treaties. Yet, significant differences in intellectual property protection levels still persist among them. Thus, the aforementioned belief is merely an illusion.
- Moreover, the level of personal information protection in a jurisdiction can be expected to change incrementally, even if the black letter law remains unchanged, due to shifts or developments in administrative practices, new judgments, and the like.

Concerns About the Current Personal Data Protection Legislation

- Assuming that the medical and health data of individual subscribers are transmitted or shared across jurisdictional borders, it is totally understandable that domestic laws, as well as subscribers, demand or expect that the provider discloses and explains the level of personal information protection in the respective relevant jurisdictions.
- However, given that the level of personal information protection continues to change as aforementioned, it is impossible to perfectly satisfy the demand and expectation for such disclosure and explanation. I don't intend to deny that the provider should make their best effort to disclose the level of personal information protection in individual related jurisdictions to potential and current subscribers.
- You cannot expect that such disclosure will always be complete or remain appropriate over a considerable period of time.
- If we insist on complete disclosure, it would become significantly difficult to provide better health services to individual subscribers using technologies and services from various countries.
- However, it also doesn't seem easy to make the domestic laws of various countries, which define personal information protection, more flexible and realistic.

Possible Solution: Dynamic Consent

- Perhaps a realistic solution would be to provide a system where subscribers' interests are reasonably protected, and they can promptly avoid inconveniences, assuming that the provider's disclosure, despite their best efforts, might be incomplete and unlikely to remain valid over time.
- Dynamic consent could be one of those possible solutions.
- By establishing a de facto standard for dynamic consent procedures, service providers from various countries could make health improvement through cross-border collaboration more feasible.



Possible Solution: Dynamic Consent

- For example,
 - To attract possible subscribers, the provider exerts their best efforts to disclose the involvement of other foreign technological components providers, AI service providers, human service providers, as well as the personal information protection levels maintained by these involved providers. The same provider also exerts their best efforts to clarify the level of personal protection ensured by foreign laws related to the service.
 - Furthermore, the provider ensures that subscribers are continually and promptly informed online about changes in circumstances, including the level of personal information protection, occurrences of incidents or accidents, and new collaboration partners. Additionally, they provide procedures that allow subscribers to give new consents online for the transmission or sharing of their medical and health data, or to opt out in the future.
 - Such information provision, as well as the opportunities for subscribers to give consent or opt out, are not conducted in a pull-based manner but rather in a push-based one, facilitated through the regular provision of an interactive user interface from the provider to the subscriber.
 - Individual subscribers engage with the services after giving consent for use and agreeing to the aforementioned procedures for information provision, continuous consent, and opting out.
 - Through such procedures, the service provider can realistically compensate for the incompleteness of information disclosure, and subscribers will likely be able to timely receive improved services and mitigate risks related to personal information protection.

Thank you.