T20 INDONESIA 2022 THINK

TAILORED APPROACH TO HEALTHCARE DATA PRIVACY IN THE DIGITAL AGE

Task Force 6

Global Health Security and Covid 19

Julien Willeme (Senior Legal Director of Data & AI, Medtronic)

Abstract

Jurisdictions around the world seek better controls to protect the privacy of their citizens' data, and adapt their laws to the "digital age," but in so doing, may inadvertently apply overly broad standards that impinge the advancement of critical healthcare goals.
In this paper, Medtronic propose a tailored international approach to health care data privacy aimed at ensuring patients benefit from the highest standards of privacy and security, while expanding access to modern digital health solutions and promoting healthcare research and innovation. This paper intends to serve as a foundation of principles upon which to build a tailored international health care data privacy framework.

Challenges

A new, tailored regime for regulating health data is needed — one that builds on the best of the current approaches to protecting patients' privacy and data security while supporting state-of-the-art digital care, research and innovation, and a variety of other social benefits in a digital age.

As individuals grow increasingly concerned unauthorized use, sharing, or selling their personal data, there is a risk — and in some countries a reality — that overly broad consumer privacy laws unintentionally sweep in health data in ways that fundamentally inhibit critical healthcare goals.

Further, in an increasingly connected world, providing healthcare and meeting patients' needs transcend regional and national borders. Data localization laws and other restrictions to trans-border health data flows constitute a major obstacle to the advancement of digital healthcare and ignore the clear benefits to countries of allowing health data to move responsibly. Duplicating servers in every country where a given medical technology is used may not be practical and it increase the risk of data breaches. At the same time, it disproportionally increases compliance costs and chills the appetite of healthcare companies, academic institutions, and foreign governments to conduct research and other activities in the territory. A new global framework must encourage and facilitate international health data flows by creating a "common framework" for responsible health data sharing centered around recognized legitimate uses, subject to appropriate safeguards.

In this paper, Medtronic will advocate for an approach built around legitimate uses of health data recognized as beneficial to patients and society at-large, and tailored regulation to prevent the harms patients are most concerned about. No current legislative/regulatory framework meets the healthcare ecosystem stakeholders' data needs fully, including the GDPR. Four years of interpreting and operationalizing the GDPR and its national derogations provides insights into what works — and what doesn't — that we think are important to share with legislators and regulators across the world who are drafting new, or refining existing, data privacy laws. This paper thus frequently refers to GDPR as a comparator for how a new data protection regime may improve upon some of the GDPR's shortcomings, while adopting its positives. This paper also makes references to the US Health Insurance Portability and Accountability Act (HIPAA) of 1996, the Singapore PDPA and the United Kingdom government's recent public consultation on the revision of the UK GDPR.

Recommendations

Proposal (1) Thinking differently about "Health Data"

A new sectoral framework for privacy regulation requires a definition of "health data" that factors in the purpose of use of the data for critical healthcare goals. The United States' health data framework, HIPAA, may provide an instructive starting point for a new definition of health data as it includes the context of the data. It includes (1) the past, present, or future physical or mental health condition of an individual, the provision of healthcare to the individual, as well as data used in the past, present or future payment for the provision of healthcare to the individual; and (2) the context in which data may be used.

Proposal (2) Recognizing "Legitimate Uses" of Health Data

We propose a privacy framework that facilitates the use of health data for specific purposes publicly recognized as legitimate with an attendant framework to protect privacy concerns, where the consent of society is presume rather than requiring individual consent. This is the approach taken by the UK Government in their recently released New Data Strategy.

A tailored health data regime must reflect the fact that health data are different from other consumer data in aim, in outcome and in legitimate use. In this paper, our focus will be to address three categories of legitimate uses of health data we believe should be distinguished from generic consumer uses: 1) Diagnosis, Treatment, and Healthcare Operations, 2) Research and Innovation, and 3) Products Safety, Efficacy, and Regulatory Oversight.

1) Diagnosis, Treatment, and Healthcare Operations

   The concept of diagnosis and treatment must be conceived broadly in privacy laws, to permit effective and timely treatment of patients and coordination of the many stakeholders involved in a patient's care pathway. Digital care pathways and telemedicine necessitate the sharing of broader data sets by an increasing number of stakeholders involved in a patient's care.

   Access to health data is also required for payment and various operational and care management activities. This includes health data access and disclosures for eligibility reviews and billing activities, which are all critical for efficiency in the healthcare ecosystem and information of payors and patients.

2) Research & Innovation

Research drives advances in technology and the digitalization of healthcare records with the aim of fueling vast improvements in healthcare access, early diagnostics, personalized treatments, diseases understanding, and developing of new treatments and medical technologies. Regulations can, at times, introduce unwarranted friction in the system and impede those improvements.

Therefore, the use and re-use of health data for research and innovation should be permitted and purposely construed under the new regime.

The new regime should specifically address opportunities in medical devices and software development, including those involving machine learning and artificial intelligence technologies that play an increasingly important role in more efficient and more personalized care.

3) Products Safety, Efficacy, and Regulatory Oversight

Regulators around the world recognize the importance of manufacturers using health data to monitor safety and product quality of their products and to conduct product vigilance. This includes well-understood methodologies and regulations which should be preserved in any new privacy regime for health data.

In that context, Real-World Data (defined as data collected in the context of the delivery of care, as opposed to data collected within a clinical trial – "RWD") provide critical opportunities for manufacturers to monitor their product's performance to identify safety signals or clinically important but statistically rare events that may not be identified in a clinical trial setting.

Once aggregated and transformed through analytics, Real-World Data becomes Real-World Evidence (RWE), whose potential applications include faster product/treatment access expansion, better safety and efficacy monitoring, faster regulatory submissions for product approvals and indications expansion.

Further, RWD access and disclosures are paramount to minimizing biases in healthcare data sets, which is now a pressing need as Artificial Leaning and Machine Learning become increasingly present in care pathways.

Proposal (3) New Privacy Framework Aligned with The OECD Privacy Principles

We propose the framework to closely mirror the OECD Privacy Principles. In this paper, we will focus on two foundational elements of the OECD frameworks: 1) Lawful basis for Processing of Health Data, and 2) International Health Data Transfers.

1. Lawful Bases for Processing Health Data

   We advocate for a privacy regime where specific health data uses are recognized as beneficial to society and therefore deemed legitimate. We provided three critical "legitimate uses of health data" earlier in this paper. Such legitimate uses should be authorized without patient's individualized consent provided certain privacy and security safeguards are in place.

   - Limitations of a consent-based system in healthcare

     Privacy laws often provide that health data collection and processing should be based on patient consent. In the healthcare setting, there are strong arguments to encourage the movement away from incident-specific consent as the default lawful basis for health data collection and processing.

     There are many instances in which a patient will not be able to provide consent to data processing, or in which repeated requests for consent from stakeholders are neither realistic nor desirable. In other instances, consent collection can only be obtained by the healthcare provider, distracting resources from the core activities of providing care.
   - Current alternatives to patient consent as a lawful basis

     Article 6(1)(f) of GDPR permits the processing of personal data where the processing activity is in the "legitimate interests" of the controller or a third party and is not outweighed by the fundamental rights and freedoms of the data subjects. Unfortunately, the very limited list of legitimate interest examples provided by GDPR has created uncertainty for organizations and data subjects alike. Therefore, the former overly rely on consent while the latter suffer from "consent fatigue".

     For this reason, we welcome the UK Government's proposal to list legitimate interests that organizations can rely upon without applying the balancing test required by GDPR, which includes product safety, internal research and development purposes. The Singapore PDPA took a similar approach by authorizing (without individual's consent) the use of personal data for research purposes, next to acknowledging legitimate interest as a possible legal basis for processing.

- Diagnostic & Treatment as a lawful basis
  We support a regime that allows health data disclosures between the different stakeholders involved in a patient's care without individualized patient consent for each use, provided certain privacy and security safeguards are in place and the patient has generally authorized uses.
  When defining permissible use relating to diagnosis and treatment, it is important to keep in mind that, with advances in mobile technologies, medical technology companies play an increasingly important role in providing patients with clinical insights related to their prescribed medical devices, thereby supporting patients in the management of their conditions. Accordingly, any regime needs to ensure that such direct-to-patient services and the related processing of health data is included in permissible use.
- Research & Innovation as a Lawful Basis
  Similar to the approach in the Singapore PDPA and the approach taken by the UK Government, we support the creation of a new, separate lawful basis for research and innovation absent patient consent. This would effectively remove barriers for researchers so that they can conduct a wide range of vital activities across sectors and geographies whilst operating within clearly defined privacy and security guardrails.
  "Research" should be defined clearly and include activities conducted by academic and governmental entities, as well as for-profit medical technology companies. For-profit companies are a critical part of the health ecosystem, translating unmet needs into products and treatments.
- Products Safety, Efficacy, and Regulatory Oversight as a Lawful Basis
  We support the creation of a new, separate lawful basis for Products Safety, Efficacy, and Regulatory Oversight absent patient consent. Data privacy laws would benefit from a uniform definition of public health activities that could be conducted absent patient consent.
  One might look to the broad interpretation of such activities under HIPAA, which includes providing reports of health information to public health authorities for the purpose of controlling disease, injury or disability and providing data to entities regulated by national authorities that ensure the safety of pharmaceutical products or medical devices to fulfill regulated activities (e.g., monitoring adverse events or post- market surveillance).

2. International Health Data Transfers

   Key privacy principles that are customized to the health data processing in the healthcare setting create a baseline of lawfulness and fairness that could span geographic borders. It will remove complexities around international data transfers and protect patient privacy rights worldwide while enabling the advancement of healthcare.

   Key privacy principles can be translated into binding commitments in a variety of ways:

   - Certification schemes and codes of conduct represent an as-yet underused, but potentially significant, tool in helping organizations to share data internationally under a uniform, approved mechanism that would be designed to reflect the unique requirements of the healthcare industry. One can envision a certification scheme and code of conduct that could achieve recognition across geographies such that it could be used to legitimize data transfers across multiple regions and countries, using as its starting point the European Data Protection Board's recently issued guidance on codes of conduct as tools for transfers.
   - Many countries already designate certain jurisdictions as having "adequate" data protection legislation. A similar pathway may be to explore sectoral adequacy decisions for health data. For example, in the U.S., covered entities and business associates subject to HIPAA may be considered adequate with respect to protected health information they hold. Similar adequacy decisions could be explored with respect to health data transferred to other countries with robust legislative regimes to safeguard health data. In the research realm, data transferred to entities that certify compliance with the international council on harmonization good clinical practice regime, including through the monitoring of research by a research ethics committee, could be considered as offering adequate protection.

References

Reference as co-chair statement.