Global Medical Technology Alliance
Innovating for a Healthier World

White Paper on Data Protection, Privacy and Global Health Data within the Medical Technology Industry

Executive Summary

In this paper, the medical technology industry proposes a more practical approach to health data protection and privacy. We believe patients deserve the highest privacy and security standards. However, without careful consideration, data protection and privacy legal requirements risk being misapplied to the health sector. Consumer-focused privacy regimes combined with restrictive data localization laws applied to the health sector will disrupt the development and supply of established and innovative medical technology products and solutions to patients and healthcare systems.

This paper proposes principles that protect individual's health data from misuse and cyber-crime, while also allowing responsible uses of that data to advance critical healthcare technologies.

This paper is not intended to be a "code" that companies adhere to, nor is it to be a detailed set of requirements. Rather, it seeks it to serve as a *foundation of global principles* upon which to build this tailored health data protection and privacy framework. These principles aim at building trust by explaining how medtech companies operate when it comes to health data. We also endeavour to "build out" sections on our "Path Forward" to provide additional details and scope.

In Section 1 (Introduction), we elaborate our rationale behind the different proposals made in this paper, and we explain how the medtech industry factors in existing data protection and privacy frameworks such as the GDPR, HIPAA, the Singapore DPDA and the planned revision of the UK GDPR[1].

In Section 2 (Thinking Differently about Health Data), we stress the importance of appropriately defining "Health Data" in the context of critical healthcare goals and make proposals leveraging the GDPR and HIPAA experience.

In Section 3 (Legitimate Uses of Health Data), we set out examples of health data uses which are beneficial to patients and society at-large and should therefore be recognized as legitimate uses and facilitated under applicable data protection and privacy laws. Those legitimate uses of health data include: (i) Diagnosis & Treatment; (ii) Research & Innovation; and (iii) Public

[1] On 18 July 2022, the UK Government presented the Data Protection and Digital Information Bill to Parliament.

Health; (iv) Administration and/or Finance Operations and Quality Improvement; (v) Product Quality and Medical Vigilance/Safety Monitoring; and (vi) Reimbursement and Outcomes Evaluation.

In Section 4 (Responsibly Sharing Health Data Internationally), we propose the creation of a "common framework" for responsible health data sharing centered around recognized legitimate uses.

Finally, Section 5 (The Path Forward for Health Data) outlines a new privacy framework specific to health data that we believe is best suited to address future opportunities and challenges in digital health.

1. Introduction

- 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 care, research and innovation in a digital age.

- No current legislative/regulatory framework fully meets the healthcare ecosystem stakeholders' data needs. To cite but one, four years of interpreting and operationalizing the GDPR provides insights into what has worked — and what has not. This experience provides important lessons for legislators and regulators across the world who are drafting new, or refining existing, data protection and data privacy laws. This paper thus frequently refers to the GDPR as a comparator for how a new data protection regime would ensure the right balance of objectives. It may also inform an interpretation of GDPR that supports critical healthcare goals, including those acknowledged by the European Health Data Space (EHDS). This paper also makes references to the US Health Insurance Portability and Accountability Act (HIPAA) of 1996, the Singapore DPDA[2] and the UK) government's recent public consultation on the revision of the UK GDPR. Data Protection and Digital Information Bill.

- As individuals grow increasingly concerned about unauthorized use, sharing, or selling of their personal data, there is a risk—and in some countries a reality—that overly broad (consumer) data protection and privacy laws unintentionally sweep in health data. In so doing, these laws fundamentally inhibit the development of life-saving research and innovation. We advocate for an approach built around legitimate uses of health data that are recognized as beneficial to patients and society at-large, and tailored regulation to prevent the harms that patients are most concerned about.

[2] Singapore Personal Data Protection Act 2012 (PDPA) is a law that governs the collection, use and disclosure of personal data by all private organisations. The Act has come into full effect on 2nd July 2014 and has been updated recently with new amendments that takes effect on 2 November 2020. Further information can be found in the link: PDPC | Amendments to the Personal Data Protection Act and Spam Control Act Passed

2. Thinking differently about "Health Data"

- A new sectoral framework for data protection and privacy regulation requires an appropriately scoped definition of "health data" that includes the purpose of the use of the data, notably the use of the data for critical healthcare goals (see section 3).

- The framework for regulating "health data" should include (1) a variety of data uses, types and sources and (2) the context in which the data may be used for secondary purposes to facilitate legitimate healthcare activities. .

    - The GDPR's approach to "data concerning health" mainly focuses on legitimizing processing in the context of "the provision of healthcare services by licensed healthcare providers." This is overly narrow, given that it may be interpreted to exclude ancillary — but important — uses of health data, such as the development of new AI algorithms for novel healthcare solutions. Moreover, inconsistent interpretations at local levels often results in highly restrictive and confusing parameters.

    - The HIPAA provides 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.

  The framework for regulating "health data" should be construed to include real-world data (RWD) and real-world evidence (RWE), which are relevant for several legitimate uses in healthcare. RWD are data relating to patient health status and/or the delivery of health care routinely collected from various sources. RWE is the clinical evidence about the usage and potential benefits, or risks of a medical product derived from the analysis of RWD. For example:

    - RWE is increasingly valuable to better understand disease and treatment, monitor device safety and efficacy, and support research and innovation. RWD/RWE are also critical to rooting out potential biases, expanding access to underserved populations, and facilitating increasingly customized, patient-centric care.

    - Beneficial applications of RWE include accelerating patient access to medical devices and diagnostics that provide earlier disease detection and more effective therapy, improving safety and efficacy monitoring, identifying better treatments for certain patient populations or conditions (taking into account for example, comorbidities), earlier reimbursement determinations to facilitate patient access, and improving health systems management.

    - Authorities that regulate medical technologies and medicines worldwide increasingly rely on RWE and RWD for regulatory decision-making and safety monitoring purposes, seeking at times cohorts from specific sub-populations.

3. Legitimate uses of health data

- Building a data protection and privacy framework for health data presumes agreement on specific publicly-recognized legitimate purposes with an attendant framework to protect data and maintain privacy— presuming the consent of society rather than requiring individual consent or absence of objection. This is also what the UK Government is exploring in its new Data Strategy.

- A tailored health data regime must reflect that health data differ from other consumer data in aim, in outcome and in legitimate use. Our focus will be to address legitimate uses of health data we believe should be distinguished from generic consumer uses:

    - Diagnosis & Treatment
    - Research & Innovation
    - Public Health
    - Payment, Operations and Quality Improvement
    - Product Quality and Medical Vigilance/Safety Monitoring
    - Reimbursement and Outcomes Evaluation

- <u>Diagnosis & Treatment</u>

  The concept of diagnosis and treatment in data protection and privacy laws must be conceived to permit effective and timely treatment of patients and coordination of the many stakeholders involved in a patient's care pathway, using the best expertise and novel technologies. Personalized care and precision medicine, digital care pathways and telemedicine necessitate the sharing of broader data sets by an increasing number of stakeholders involved in a patient's care, sometimes across several countries.

- <u>Research & Innovation</u>

  Research is the key element that drives advances in technology and the digitalization of healthcare records. Research drives these advances in many ways, including enabling vast improvements in healthcare access, improving diagnostics and treatments, enhancing detection, advancing our understanding of diseases, and developing new treatments. Privacy regulations are often targeted to address consumer issues, and are not as focused on medical research, leading to unnecessary friction or direct conflicts that impede medical research's ability to deliver on its potential.

  Therefore, the use and re-use[3] of health data for research and innovation should be permitted without any specific authorizations and purposely construed under the new framework.

  The new framework should specifically address opportunities in medical devices and software development, including those involving artificial intelligence (AI)

[3] In this context, the re-use of health data means the possibility for the manufacturer of medical technologies to re-use personal data collected via its medical technologies for research and innovation purposed to improve the products and solutions, subject to appropriate safeguards and the applicable legal framework.

technologies and other sub-sets of AI such as machine learning that play an increasingly important role in delivering more efficient and more personalized care, through the re-use of other patients' health data.

- Public Health

  The ability to use data for public health reasons remains critical. Health data use and sharing in the response to the COVID-19 pandemic is instructive, but the new framework requires a wider application and should also encompass (1) developing products and services that could protect individuals' health and wellbeing, (2) innovation activities that promote public health, and (3) submissions to competent regulatory authorities with oversight functions of medical technologies and medicines. While recital 54 of the GDPR provides a broad description of 'public health', it remains unclear when art. 9, par. 2, (i) applies.

- Finance and/or Administrative Operations and Quality Improvement

  As well recognized by the HIPAA model, the Singapore Advisory Guidelines for the Healthcare Sector, and within other country laws, access to health data are required for financial or other various operational and quality improvement activities. Access to health data for payment purposes, such as eligibility reviews, billing activities, and risk adjustments, is critical for efficiency in the healthcare ecosystem and timely and comprehensive information for payors and patients. Likewise, heath data are used by healthcare providers, health insurance plans, medical device and diagnostics manufacturers, and other contributors in the care pathway to manage and improve their services. Such activities include quality assessments, clinician competency reviews, and the development of more sustainable healthcare systems.

- Product Quality and Medical Vigilance/Safety Monitoring

  Sectoral regulators around the world have long recognized the importance of manufacturers using health data to conduct product vigilance and broader post-market surveillance to detect and report adverse event, monitor the product's safety and effectiveness, identify trends, monitor product quality, and comply with other regulatory obligations. This includes well-understood methodologies and regulations which should be preserved in any new data protection and privacy framework for health data. RWE/RWD and other digitized health data provide expanded opportunities for manufactures to monitor their product's performance to identify safety signals earlier (but also vulnerabilities) or opportunities to improve outcomes before the occurrence of incidents. For example, RWE/RWD will help identify clinically important but rare events that may not be clearly tied to a specific device or treatment pattern or are sufficiently rare that they could not reasonably be identified in a clinical trial setting, e.g., genetic data.

- Reimbursement and Outcomes Evaluations

  Health data are critical for the purposes of pricing, reimbursement, and procurement by national health authorities, insurance plans, hospitals, and laboratories. More and more, governments, tendering authorities, and hospitals are looking at value-based healthcare (VBHC) models and, more generally, the overall effectiveness and cost of medical services. Health data, responsibly curated and protected in a secure environment, are critical to meeting these important goals.

4. Responsibly Sharing Health Data Internationally

- In an increasingly connected world, providing healthcare and meeting patients' needs transcend regional and national borders. This was recognized again recently by the European Commission's initiative to create a European Health Data Space that should enable free flow of health data across the European Union. A new global framework must encourage and facilitate international health data flows by creating a broadly accepted framework for responsible health data sharing centered around recognized legitimate uses, subject to appropriate safeguards (see section 5, chapter G). Well-founded, beneficial uses that involve sharing health data internationally include:

    - Patients regularly travel and receive treatment across borders, and their health data must be able to follow them. Uninterrupted data flows are required for this to be done safely, secure, and effectively.

    - Clinical trials are no longer state- or country-specific. Regulatory bodies such as the U.S. Food and Drug Administration and the European Medicines Agency emphasize the importance of multi-regional clinical trials. The viability of such trials depends on the ability of all stakeholders to access and share data across countries.

    - Product Safety Data. Reports of product adverse events are typically triaged on a country or regional basis. Minimal information is transferred globally for purposes of case analysis and reporting to competent health authorities.

    - Precision Medicine, Personalized Care, and Product Customization. Precision medicine involves tailoring disease prevention and treatment, taking into account differences in people's genes, environments, and lifestyles. The goal of precision medicine is to target the right treatments to the right patients at the right time. Sharing health data is essential to developing, operationalizing, and advancing certain precision medicine therapies. Extending from this concept, there is an increasing trend to customize therapy to meet patients' unique needs, e.g., sizing services, individually customized, 3D-printed implants, therapies for rare diseases, etc. Product customization and precision medicine services may require the transfer of more directly identifiable information.

    - Remote Support Services. The support, maintenance, and repair of today's highly sophisticated medical devices often require specialized knowledge and training and must be made available 24/7 on a global basis. Remote servicing such as providing hardware and/or software system support, maintenance and troubleshooting, may need to be organized centrally or regionally, across borders or overseas, requiring the sharing of certain health data internationallhy. Remote servicing capabilities have become common for most IT-based medical equipment because they can monitor system performance and diagnose issues more efficiently, , enabling earlier detection and correction of potential problems that could compromise the proper operation or continued availability of the device. Sharing device data, which can include patient health data, with remote technicians may be required to assess the nature of the issue and determine possible who should be deployed to repair the device.

    - Telemedicine and Remote Care Coordination. Expanded patient access to care through telemedicine and improved health outcomes through remote care

coordination have only been possible because of the free flow of health data across country lines. Increasingly, expert clinicians located in one country advise on surgeries performed abroad. The availability of these platforms to reach and benefit patients will be curtailed if these data flows and uses are not factored into to new data privacy and security laws and regulations.

- The use of RWE/RWD requires pooling data sets from multiple jurisdictions to analyze trends and, ultimately, benefit patients with the advances that emerge from such exercises. Limiting such data to regional/national borders impedes the ability to identify the benefits and risks of medical technologies, increases the likelihood of introducing bias in RWE datasets, and needlessly drives healthcare costs up.

- Data localization laws and other restrictions to cross-border health data flows should be strongly resisted. Such trends ignore the clear benefits to countries of allowing health data to move responsibly. Moreover, the use of centralized servers may be preferred to ensure maximum investment in secure data hosting solutions. 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 beneficial activities in the territory, further compounding the lack of in-country development and innovation for healthcare.

5. The Path Forward for Health Data

- In this section, we outline a new data protection and privacy framework specific to health data that we believe is best suited to address the opportunities and challenges set out in sections 1 to 4 of this paper.
- Our proposed framework largely mirrors the OECD Privacy Principles and is structured around the following principles:

A. Lawful basis for Processing of Health Data

B. Openness and Transparency

C. Security Safeguards

D. Data Minimization

E. Individual Participation

F. Accountability

G. International Health Data Transfers

A. Lawful Bases for Processing Health Data

The starting point is recognizing that there are legitimate uses of health data that society recognizes as beneficial and should therefore be deemed authorized. Section 3 of this paper discussed critical "legitimate uses of health data". Such legitimate uses should be

deemed authorized without obtaining a patient's individualized consent provided that certain data privacy and security safeguards are in place such as pseudonymisation and encryption.

- Limitations of a consent-based system in healthcare

  Data protection and privacy laws often provide that health data collection and processing should be based on patient consent. In the healthcare setting, there are compelling justifications to move away from treatment-specific consent as the default lawful basis for health data collection and processing.

  There are many instances where a patient will not be able to provide consent for data processing associated with medically necessary diagnostics, therapeutics, or monitoring. In other instances, repeated requests for consent from various technology providers whose products may be involved in a treatment episode are neither realistic nor desirable. For example, an individual presenting with a heart attack may interact with more than a dozen different technologies to diagnose and treat the condition—e.g., diagnostics in the ambulance, vitals, electronic medical records, electrocardiogram, echocardiogram, pulse oximetry, fluoroscopy, anesthesia machine, implanted device to maintain proper heart function, and many more. Furthermore, repeated consent could burden the very sick or elderly. In many instances, a medtech company will have no direct interface with the patient so consent can only be obtained by the healthcare provider. Requiring clinicians to obtain consent for each data collection, use, and transfer necessary for care would be wasteful, consuming their limited, valuable time without an accompanying benefit to the patient or society.

- 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, and the lack of a corresponding exception in Art. 9, par. 2 of GDPR have created uncertainty for organizations and data subjects alike. As a consequence, organizations overly rely on consent while the data subjects from "consent fatigue". 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. For this reason, we welcome the UK Government's proposal to have a list of recognized legitimate interests that organizations can rely upon without applying the balancing test required by GDPR.

  A slightly different but also useful sectoral approach is provided by HIPAA. HIPAA permits a broad range of uses of health data for purposes of treatment, payment, or health care operations following a simple and broad privacy notice to patients (and without requiring individual consent). Individual authorization is required only for additional uses (outside of the treatment, payment, and healthcare operations purposes) such as direct marketing or the selling of patient data. Better still, HIPAA details how organizations must craft the authorization content, which increases consistency and clarity. Notably, lawmakers in the United States have recognized the effectiveness of this approach and have been reluctant to change it.

- Diagnosis & Treatment as a lawful basis

    - Overarching Principle

      We support a regulatory framework that allows health data disclosures between the different stakeholders involved in a patient's care without individualized patient consent for each use, provided certain data protection and privacy and security safeguards are in place and the patient has generally authorized uses. HIPAA enables and facilitates these types of disclosures. We will expand on possible privacy and security safeguards in chapters B to G below.

      When defining permissible use relating to diagnosis and treatment, it is important to keep in mind that, with advances in wireless technologies (e.g. 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 remote management of their conditions. Accordingly, any framework needs to ensure that such direct-to-patient services and the related processing of health data is included in permissible use.

    - Professional Secrecy

      Jurisdictions where medical professionals are bound by domestic statutory, regulatory, or professional secrecy obligations should be factored into new data protection and privacy laws. New regimes should permit the processing of health data all such individuals involved in a patient's care, subject to specific safeguards. This would broaden patient access to care via telemedicine and other digital health technologies by enabling appropriately licensed health care professionals (and other authorized suppliers) located in jurisdictions other than the patient's to access the patient's health data. Expansion to healthcare providers in jurisdictions that lack professional secrecy obligations can be accomplished through contractual obligations for confidentiality.

      That clarification would be particularly useful in the GDPR context. Article 9 (2)(h) of the GDPR allows for the processing of health data where the provision of treatment and management of healthcare services is done based on, or under a contract with, a healthcare professional that is subject to professional secrecy obligations provided by country law. That limitation has frustrated the ability of patients to receive care from leading health care providers who are located in other jurisdictions.

- Research & Innovation as a Lawful Basis

    - Overarching Principle

      Similar to the approach in the Singapore PDPA, we support the creation of a new, separate lawful basis for research and innovation with appropriate controls so that patient consent would not be needed. This would effectively remove barriers for researchers so that they can conduct a wide range of studies across sectors and geographies while operating within clearly defined privacy and security guardrails. Chapters B to G will expand on possible data protection and privacy and security guardrails.

- Defining "Research" and Innovation

  Research should be defined broadly 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.

  Notably, the GDPR does not contain a definition of "scientific research". Nonetheless, it encourages a broad interpretation of scientific research that extends to the areas of "privately funded research" and "technological development" (see Recital 159). On the other hand, this makes it hard for researchers and patients to understand when the GDPR research regime applies as there are a lot of ambiguities with regard to their legal obligations and rights. The UK Bill provides a statutory definition, based as a starting point on Recital 159 of the UK GDPR, including processing for the purposes of technological development or demonstration, fundamental research or applied research. A broad definition of research is required, allowing for different types of research, without limiting research to 'research in the meaning of the Declaration of Helsinki; this would include clinical trials, patient surveys, but also the development and improvement of new or existing medical devices or therapies, the development and improvement of device guidelines, and health economics and clinical outcomes research. This definition should represent a key pillar in the new global framework sectoral regime.

  One might look to the following definition found in the U.S. Common Rule and HIPAA, but modified to include expressly the bolded language that focuses on product development and improvement activities, including through use of artificial intelligence and machine learning *i.e.*, a systematic investigation, including *research development, testing and evaluation, designed to develop or contribute to generalizable knowledge,* ***including research to develop new products or improve existing products, including through use of artificial intelligence and machine learning***. The list should also include data processing for the purpose of detecting bias and improving care pathways and outcomes, given that such activities clearly fall within the legitimate interests of stakeholders across the healthcare value chain.

- Lawful Basis in Public Health and Implications for Real-World Evidence

  Similar to Research, we support the creation of a new, separate lawful basis for Public Health absent patient consent. Data protection and 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).

This latter activity should be defined explicitly to include the processing of personal data for RWE/RWD applications which we provided a few examples of in Section 3 of this paper. As we showed, the advances in and importance of RWE/RWD are central to the development of a new harmonized framework for health data that benefits patients and providers alike. Existing data protection and privacy laws do not specifically reflect the importance of utilizing RWE/RWD to (for example) support the health technology appraisal of a medical device by governmental or private payors that make reimbursement decisions. The data that result from any reimbursement in conjunction with such appraisal should also be specifically permitted under a new harmonized framework.

- Concept of "compatible" data processing

  Because health data collected for one purpose (e.g., patient treatment) may be valuable for secondary purposes, such as research or public health activities, it would be beneficial to borrow from Article 5(1)(b) of the GDPR the concept that personal data may be processed for purposes that are "compatible" with the initial purposes of processing without first establishing an additional basis for processing. With respect to health data, compatible purposes should be defined broadly to include research, public health interest and product development purposes.

- Broad authorization & legitimate health data uses

  When authorization or consent is used as the basis for processing, as may be the case in clinical research in which there is a strong tradition and practical opportunity of obtaining patient consent, individuals should be permitted to authorize a broad range of future uses that may not be possible to fully describe at the time of data collection, such is the case of utilization patient health data for creating synthetic data, patients digital twins, etc..

- The divergent approaches to the availability of such broad consent in the EU and UK have stymied research. One might adopt the standard set forth in HIPAA for the authorization for future research, which permits a patient to provide an authorization for unspecified future research provided that the activity is defined with enough specificity such that it would be reasonable for the individual to expect that his or her health information could be used or disclosed for such future research. The UK new strategy on data contemplate the same type of approach — but we suggest that a similar framework could also be applied to consent for other, non-research uses like product development or public health purposes.

B. Openness and Transparency

- The principle of transparency is essential. Companies processing health data for their own purposes should be bound to inform patients and others how they may use data. However, granular, individual-level disclosures to patients are highly impractical and at times impossible, especially for organizations that do not directly collect their personal data. This will often be the case in a medical device ecosystem where health care providers act as intermediaries between a patient and a medical device manufacturer.

- While data protection and privacy laws (such as art. 14 of the GDPR) may provide exceptions to transparency requirements when they would come at a disproportionate effort, not all data protection and privacy laws do. Exceptions to transparency requirements could be broadened, for example, (i) where processing relates to public health interest or similar purposes and data are not collected directly from the data subject, and (ii) with respect to further processing for secondary research purposes where the data are initially collected *directly* from the data subject, subject to removal of direct identifiers. The UK Bill provides a good first step by allowing for an exception to notify when the controller intends to further process the personal data for scientific research purposes (subject to safeguards) and providing the information is impossible or would involve a disproportionate effort.
- Companies should also be allowed, where an exception would not apply, to provide transparency information on a non-individualized basis (such as via a general website privacy notice) without violating these transparency requirements.

C. Security Safeguards

- A principles-based framework, like that found in Article 32 of the GDPR, which permits one to scale the security measures based on the risk presented by the processing activity, may provide the most flexibility to organizations processing health data. This should include safe harbors using agreed-upon security standards, such as a NIST framework, NIS and NIS2 in Europe, and the international consensus standards on IT and data security.

- As an alternative, one might consider adopting a framework that contains more precise security standards, such as the HIPAA Security Rule.

D. Data Minimization

- Data protection and privacy regimes generally permit more flexible uses of data that have been de-identified or anonymized such that they are no longer considered "personal data" under the relevant legal regime.

- One challenge posed by the GDPR is that it continues to apply to "pseudonymized" data even when held by an entity that lacks the key or additional information needed to re-identify the data subject.

- An alternative approach that could increase the utility of health data while continuing to safeguard data subjects would be "relative anonymization," in which anonymization is judged by the ability of the party holding the data to re-identify the data subject. Under this approach, data could be considered reasonably "anonymized" and thus no longer subject to data protection law if held by a party lacking the means to re-identify the data subject, provided that adequate technical and organizational measures are in place to prevent re-identification (e.g., contractual arrangements prohibiting the party

holding the key needed to re-identify the data subject from sharing the key with the party holding the data)[4].

- Finally, a much more balanced and risk-based framework is required to improve effectiveness in practice. According to Hunton & Williams a "*The risk-based approach goes beyond mere compliance with regulatory requirements. It goes to the heart of what responsible and accountable organisations seek to achieve, how they implement privacy requirements on the ground and how they demonstrate compliance.*". no inference concerning an individual. A purely academic risk of re-identification following the removal of many, but not all, patient identifiers should be balanced against the value of using the data to the patient data subjects themselves, broader patient populations, and the healthcare system.

E. Individual Participation Principle

- Data protection and privacy laws increasingly provide data subjects with robust rights with respect to personal data concerning themselves (e.g., the right of access, amendment and accounting under HIPAA, and rights of access, rectification, restriction, erasure and portability under the GDPR).
- In certain contexts, such as patient care, there are strong policy arguments in favor of providing such rights as they support patients managing their conditions.
- In other contexts, such as research or public health, the exercise of certain rights, such as erasure or restriction on processing, may frustrate or render impossible the purpose of the processing activity. More difficult is the panorama for manufacturers of medical technologies that need access to health data for their own research and development activities. The GDPR recognizes this by providing in Article 89 a framework for EU Member States to limit data subject rights when the exercise of such rights would render impossible or seriously impair research or archiving in the public interest. At the same time, permitting Member State variation has limited the utility of this provision of the GDPR.
- A better approach would be a data protection and data privacy framework in which data subjects' rights concerning health data are limited uniformly when they would disrupt research or public health activities, and/or if this would oblige companies to keep identifiers that are not needed for the research or other legitimate purpose/s. This may be coupled with principles that limit data to what is necessary for the research purpose, and use data minimization and related techniques to address data protection and privacy considerations.

F. Accountability

- Given the complexities of harnessing health data described throughout this paper, and the patchwork of national laws that govern these data, a global accountability mechanism should be developed that encourages the use of research data while retaining the controls that ensure data are collected, shared in secure environment and used lawfully.

[4] A Risk-based approach to Privacy: Improving Effectiveness in Practice, Centre for Information Policy Leadership, Hunton & Williams LLP, 19 June 2014

- This risk- and principles-based accountability framework — which could be designed in conjunction with codes of conduct and/or certification schemes referenced in chapter G below — would draw on the best of current approaches to regulatory decision-making and approval, security and data use to help researchers, national health services and governments unlock the power of health data within a transparent and secure structure.
- Companies should be required to have robust privacy compliance programs, for instance in the form of a data governance board that sets standards for how and when health data are used under compatibility or legitimate interest provisions. A compliance program could include company policies and procedures, role-based access, control measures, monitoring and auditing, and efforts to build a culture of privacy within the organization.

G. International Health Data Transfers

- Key data protection and privacy principles, in combination with security measures, that are customized to health data processing in the healthcare setting create a baseline of lawfulness and fairness that could span geographic borders. That baseline would remove complexities concerning international data transfers and protect patient privacy rights worldwide while enabling the advancement of healthcare. International consensus standards on IT security will ensure secure international health data transfers.

- Key data protection and privacy principles can be translated into inherent 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 while enabling the assessment and demonstration of compliance with global data protection and privacy laws[5]. Using the European Data Protection Board's recently issued guidance on codes of conduct as tools for transfers as a starting point, one can envision a certification scheme that achieves recognition across geographies such that it would be used to legitimize data transfers across multiple regions and countries.

As additional countries worldwide follow the GDPR's approach of designating certain jurisdictions as having "adequate" data protection legislation, an additional 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 the protected health information they hold. Similar adequacy decisions could be explored concerning health data transferred to other countries with robust statutory/regulatory 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.

[5] The Governance of Privacy Through Codes of Conduct: International Lessons for U.S. Privacy Policy by Colin Bennett, Deirdre K. Mulligan :: SSRN