Position Statement on Responsible Uses of Technology and Health Data During Times of Crisis for the Future of Privacy Forum

Title: IoMT and Data Protection Challenges during the COVID-19 Pandemic

Author: Lyz Veronica Llamas Vallejo

Affiliations: Senior Privacy Counsel at FIRST PRIVACY GmbH

Contact Information: Lyz Llamas Vallejo, MLB

Senior Privacy Counsel / Senior Beraterin Datenschutz

E-Mail: lllamas@first-privacy.com

Tel: +49 (0) 421 69 66 32-883

IoMT and Data Protection Challenges during the COVID-19 Pandemic

Due to the developments of the current COVID-19 world pandemic, there has been an explosion of the so called interconnected objects or the "Internet of Things", which has derived into the need to regulate the data processing operations carried out through these objects. Even more so in relation to "sensitive data" and in particular to the data related to people's health, through the development of devices classified within the Internet of Medical Things (IoMT). The development and use of IoMT devices during the COVID-19 world pandemic has led to their accelerated evolution in order to cover diverse needs[1] such as telemedicine, and the prevention of spread of the disease, for example to avoid further exposure of the medical staff when treatment is taking place.

The demands of the medical and health sector in regards to the development and implementation of IoMT devices to satisfy their diverse needs necessarily involves the processing of health data. Therefore, the protection of personal data in particular under the European Scope of the General Data Protection Regulation (GDPR), is an essential element that should be intrinsic to their evolution and requires further reinforcement by integrating the data by design and by default, into their regular development process. The COVID-19 pandemic has proven to be a challenge for this integration as development teams seek to solve issues quicker and data protection concerns are challenging to their accelerated needs. Therefore, a framework of standardized data protection requirements for these devices under the GDPR should be developed to meet these needs.

As a result of the above integration, the following requirements could constitute a gateway for the standardized requirements:

1. Since health data is being processed by IoMT devices as this is within the nature of their functionality, there will always be a need to conduct a data protection impact assessment (DPIA) according to Article 35 of the GDPR. The level of risk emanating from the processing of these types of personal data categories involves a high risk to the privacy of the data subjects. This is why impact assessment should be part of the design of IoMT devices.
2. The specific conditions of the data subjects also play an important role when establishing the level of risk in regards to a processing operation and how the different obligations are met with respect to each category of data subject. That is to say, depending on their capacity and role within the treatment, the design of the fulfillment of the different obligations before each one of them should be addressed.
3. When assessing the legal basis applicable to the processing of personal data by means of IoMT devices, they may be replicated for most processing operations. In which case, the legal basis for the processing operations may be carried out based on the exceptions of consent and vital interest of the data subjects under article 9 of the GDPR. These will then most likely always be mirrored within the data protection impact assessments.
4. The duty of transparency will also constitute an essential element in the development of IoMT devices. Within the design of the device, the essential information to be provided to each category of data subject must be considered in compliance with the GDPR. It will therefore depend then on the specifics with respect to the functionality and purposes of the specific device and processing operation, to design an effective strategy that guarantees the duty of information on the treatment according to the principle of transparency.

[1] Gerke, S., Shachar, C., Chai, P.R. *et al.* Regulatory, safety, and privacy concerns of home monitoring technologies during COVID-19. *Nat Med* **26,** 1176–1182 (2020). https://doi.org/10.1038/s41591-020-0994-1

5. Finally, the technical and organizational measures (TOMs) concerning IoMT devices should not be overseen even in the development of a world pandemic[2], they should be deployed according to the risks of the operation. As previously established, the processing operations carried out through IoMT devices will most likely involve the processing of personal data related to health, therefore the technical and organizational measures should be congruent with the processing of high risk operations. Having already, then the TOMs to be implemented should reduce the risk of the processing operation. These measures must be guaranteed throughout all stages of the processing, from the moment of collection to the moment of deletion of the personal data involved.

The above elements could constitute a base to clarify the minimum standards for data protection compliance in the context of IoMT devices. In which case the integration of the above measures within the design of these devices would serve the purpose of developing a format that would allow for the acceleration of the development and compliance with data protection standards from design and by default of these devices. The above proposition is also inspired in the Toolkit developed by the European Commission in regards to the development of mobile apps to support the fight against the world pandemic[3]. In this case the proposal is to unify the elements that should be integrated in the design stages of IoMT devices so that it is clear from a technical and legal aspects which data protection implications need to be addressed in order to accelerate their adaptability and compliance, two of which have proven to be essential requirements in the use of technology against the pandemic.

[2] Vassilis Karantounias and f Cynthia O'Donoghue, COVID-19 Questions & Answers Coronavirus emergency vs. GDPR security standards, April 10, 2020.
[3] European Commission, COMMUNICATION FROM THE COMMISSION Guidance on Apps supporting the fight against COVID 19 pandemic in relation to data protection, 16.04.2020.