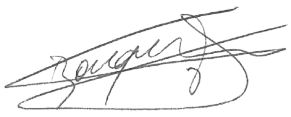
Declaration of Compliance with the GPDR

In accordance with the principle of transparency established by the European General Data Protection Regulation (GDPR), the MultiHealth Group (MTH) and its subsidiaries (hereinafter referred to as "We", "Our") have written this document. Its purpose is to describe the various technical and operational measures put in place to ensure compliance with the GDPR with regard to the processing of personal data by Us.

This document will be limited to the provisions that We take as a clinical research provider.

Version	Reason of modification	Date	Author
1.0	Document creation	01/31/2020	Jaufret BOUQUET
1.1	Minor update	02/12/2020	Jaufret BOUQUET

DPO	DPO Assistant	Approver
Dr Gérard SORBA President of the Group MTH Date : 02/12/2020	**M. Jaufret BOUQUET** Developer Date : 02/12/2020	**Mme Florence CARRÈRE** Head of technical operations Date : 02/12/2020
		

Contents

1 Information of the data subject about the processing of these data

In accordance with Article 13 of the GPDR, data subjects are informed, inter alia, of the personal data concerning them (including medical data if applicable) that will be processed by Us. This information, as well as the other elements imposed by article 13 of the GPDR, are included in the Terms of Service (TOS), which are publicly accessible for our various applications.

For some of our applications, the data subjects will have to confirm that they have read and unreservedly accepted the said TOS in order to be able to continue to use the said applications.

2 Treatment safety

According to Article 32 of the GPDR, the controller and the processor must take technical and organizational measures to ensure the ongoing confidentiality, integrity, availability and resilience of their processing systems and services.

As indicated in our TOS and in our service contracts, all the healthcare data that We process are hosted by a specialized service provider, Cegedim, whose servers are located in France. In accordance with Article L.1111-8 of the French Public Health Code, as amended by Law No. 2016-41 of January 26th, 2016, these servers are HDS certified (Health Data Hosting). This is a certificate issued by the French Ministry of Health that certifies that the health data that We process are hosted in security conditions adapted to their criticality.

In addition to the HDS certification, our hosting provider has the following certifications related to the management and security of assets and IT systems:

- ISO 2000-1: 2018 ;
- ISO 27001: 2013 ;
- ISO 27017: 2015 ;
- ISO 27018: 2014.

Each connection to the servers and each action are recorded in a log by our hosting provider. We have a read-only access to this log.

2.1 Guarantees of confidentiality

2.1.1 Pseudonymisation

The pseudonymization of patients managed via Our applications is guaranteed by the allocation of a generically determined inclusion number. As Clinical Research Associates (CRAs) have access to patient records, they are subject to professional secrecy (formerly medical secrecy), in accordance with article 4.14 of the GCP, code R5121-13 of the French Public Health Code, and articles 226-13 and 226-14 of the French Penal Code.

2.1.2 Access and encryption

Access to these applications is protected by a strong login/password combination (renewed frequently), and is via a TLS encrypted connection (managed by our specialist service provider). In the event of a certain number of connection attempts, the account is blocked and the password must be changed. Only the study administrators can create, activate and deactivate the accounts of the study participants. Only one session per user is accepted, and this session is automatically closed after a certain period of inactivity.

At the end of the study, the encrypted data are transmitted to the client (by default in AES-256) on a physical medium, and the encryption key is provided separately. After acknowledgement of receipt and integrity check of the data by the customer, the data are definitively destroyed from our servers, and a certificate of destruction is issued.

2.1.3 Minimization and Partitioning

Only the medical data necessary for the purposes of the research carried out are collected, in accordance with the CNIL's Reference Methodology MR-001, based on Declaration No. 2018-153 of May 3rd, 2018.

By default in our applications, patient data are compartmentalized by center and are not accessible to administrators. This is made possible by a system of rights that also compartmentalizes the scope of data that can be consulted by the user on the basis of his/her profile, or specific rights that can be assigned or revoked.

2.1.4 Malware and Intrusion Control

Our computer network is protected by a physical firewall and each computer workstation is equipped with antivirus software that is daily updated. Users do not have administrator privileges. Indeed, our computer network is managed by a qualified subcontractor. Regularly, another service provider expert in computer security audits our systems.

2.1.5 Security of the premises

Our facilities are located in a business park closed during non-working hours and days, with a permanent guard, video surveillance and perimeter alarm.

Our facilities are constantly under video surveillance. Each access to the building can only be done via a name badge, or after the reception has opened the main door. To access the stairs from the reception desk or to operate the lifts, the name badge is again required.

Our offices are protected by an anti-intrusion alarm that can be activated and deactivated by name, and managed by a remote surveillance company.

The room of our internal server (containing no health data), firewall or access control system is only accessible to a very limited number of Our employees. It is permanently under video surveillance and fire surveillance.

2.1.6 Records of processing activities

In accordance with Article 30 of the GPDR, we have setup a Register of Our processing operations recording the following information:

- The name and contact details of the data controller, as well as those of his DPO;
- The purpose of the processing operation;
- A description of the categories of data subjects;
- A description of the categories of personal data processed;
- A category of possible recipients;
- In case of transfer outside the EU or to an international organization: a list of data security safeguards;
- If possible, the retention period of the categories of data;

- If possible, a general description of the security and organizational measures taken;
- The name and contact details of each processor (and their DPO if applicable);
- The categories of processing operations carried out on behalf of each controller;
- In case of transfer from processors outside the EU or to an international organization: a list of data security safeguards;
- If possible, a general description of the security and organizational measures taken by the processor.

2.1.7 Data protection impact assessment

In accordance with section 35 of the GPDR, we have established an impact assessment plan. This plan identifies in detail the existing data processing operations, the regulatory aspects surrounding these processing operations, as well as the potential impact on the privacy of the data subjects in case of a data breach as defined in Article 4 of the GPDR.

2.2 Guarantees of integrity

2.2.1 Servers access

Access to the servers containing the health data is done *via* SSH protocol, inside a VPN tunnel. Access is personal and must be requested in writing to our provider. It is also subject to the signature of a charter reminding the obligations of users with HDS access. Authentication is said to be strong, and passwords or encryption keys are renewed periodically.

Each study that We host has its own database (partitioning). The databases are protected by strong passwords.

2.2.2 Data backup

As contractually defined, a data backup is automatically performed every six hours. Each backup is kept for a rolling 60 days period. The backups are performed and held by our hosting provider.

2.2.3 Logging

Each connection to Our applications is logged in Our Apache server by Our hosting provider.

Our applications log all data entry, modification, deletion or monitoring of medical data, as well as certain study management actions. This log includes, among others:

- A personal timestamp;
- A description of the action;
- The value before and after modification.

2.3 Availability guarantees

The availability of our applications is driven by two factors:

- The availability rate of our hosting provider's servers;
- The maintenance operations that we carry out and which require a partial disruption of services.

The availability of the servers is contractually guaranteed by Our hosting provider up to 99.98%. As for maintenance operations requiring a partial interruption of service, these remain very occasional.

All data and their backup are replicated on other HDS servers of our hosting provider. These servers are located in France, more than 150 km away from the first ones, in order to protect against geological or nuclear risks.

2.4 Resilience guarantees

Contractually, our hosting provider undertakes to resolve a service interruption within four working hours.

As for us, we have a business continuity procedure aimed at a minimum business resumption in three days in the event of a major disaster (total unavailability of the premises).

3 Data protection by design and default data protection

Our clinical research management applications are designed in-house by qualified developers, one of whom is a DPO. In this way, we meet the obligations set out in Articles 24 to 25 of the GPDR to oversee the design of systems that process personal data from the outset.

4 Subcontracting

4.1 As a client

In accordance with article 28 of the GPDR, in the event that We call upon a subcontractor to carry out the clinical research entrusted to Us, one of our procedures consists in asking Our provider to produce an attestation of compliance with the GPDR.

4.2 As a subcontractor

In accordance with article 28 of the GPDR, as a subcontractor, we have a DPO and a procedure to make Our employees aware of the provisions of the GPDR, in order to be able to offer our clients advice and services that comply with this regulation.

4.2.1 Joint definition of the purposes of treatment

According to Article 26 of the GPDR, joint responsibility exists where the purposes of the processing operation are jointly defined by the controller and the processor. These responsibilities are determined by the sub-contracting agreement that We sign with our client, as well as by the FIU serving as the specifications.

5 Notification of violations

In accordance with Articles 33 to 34 of the GPDR, and in the event of data breach, we have to follow the procedures mentioned below:

- Procedure for notifying the controller;
- Procedure for notifying the authorities;
- Procedure for notifying data subjects;
- Procedure for remedying the problem.

6 Exercise of data subjects' rights

In accordance with Articles 15 to 22 of the GPDR, data subjects have various rights regarding their personal data and related processing. To allow for the exercise of these rights, the following procedures have been put in place:

- Procedures for acknowledging receipt of requests from data subjects;

- Procedure for exercising the right of access;
- Procedure for exercising the right of destruction;
- Procedure for exercising the right of restriction (including the lifting of the restriction);
- Procedure for exercising the right of portability;
- Procedure for exercising the right of objection.

7 Transfer of data outside the EU or to an international organization

In accordance with Articles 44 to 49 of the GPDR, we have the following procedures in case we need to transfer personal data outside the EU or to an international organization:

- Procedure for verifying whether the country concerned is on the white list;
- Procedure for requesting guarantees from the customer;
- Procedure for derogation from Articles 45 and 46 of the GPDR.