Protection of Personal Data relating to the QUARTZ Program

QUARTZ Program is compliant with the most restrictive international rules on the protection and use of personal and medical data.

1) **QUARTZ program is 100% compliant with Regulation (EU) 2016/679 known as the EU General Data Protection Regulation (GDPR)**

As of May 2018, with the entry into application of the General Data Protection Regulation, there is one set of data protection rules for all companies operating in the European Union (EU), wherever they are based. GDPR regulates the processing by an individual, a company or an organisation of personal data relating to individuals in the EU.

If you need more details:

https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en

https://www.eugdpr.org/

2) **A Data Protection Officer (DPO) had been appointed for QUARTZ Program (cases b and c)**

DPOs must be appointed in the case of: (a) public authorities, (b) organizations that engage in large scale systematic monitoring, or (c) organizations that engage in large scale processing of sensitive personal data (Art. 37).

3) **QUARTZ Program is 100% compliant with EU Health data protection and the French Public Health Code (Article L.1111-8) known as "Hébergeurs de Données de Santé" (HDS).**

Health data refers to personal information (also called personal data) that relates to the health status of a person. This includes both medical data (doctor referrals and prescriptions, medical examination reports, laboratory tests, radiographs, etc.), but also administrative and financial information about health (the scheduling of medical appointments, invoices for healthcare services and medical certificates for sick leave management, etc.). Health data is considered sensitive data and is subject to particularly strict rules and can only be processed by health professionals who are bound by the obligation of medical secrecy. Furthermore, the organisation shall take the necessary security measures to ensure that the health data is protected and not subject to any unauthorised disclosure.

The French Public Health Code requires that services providers hosting certain types of health / medical data (HDS) be accredited for this activity.

The HDS' personnel are bound by professional secrecy obligations. The HDS cannot use the data for any other purpose nor sell the data, even with the data subject's consent. It has to return the data at the end of the services. The HDS does not need to host the data in France.

After 1 April 2018, the HDS must be certified by an accreditation body authorised, in France by the COFRAC and, in the EU by the national equivalent of the COFRAC. The certification process and other regulatory requirements have been enacted by a Decree of 28 February 2018 (the "Decree") which created, effective 1 April 2018, new articles R1111-8-8 to R1111-11 of the Public Health code.

4) **QUARTZ Program is 100% compliant with other national regulations like the Health Insurance Portability and Accountability Act (HIPAA) in US**

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) required the Secretary of the U.S. Department of Health and Human Services (HHS) to develop regulations protecting the privacy and security of certain health information.1 To ful fill this requirement, HHS published what are commonly known as the HIPAA Privacy Rule and the HIPAA Security Rule. The Privacy Rule, or Standards for Privacy of Individually Identifiable Health Information, establishes national standards for the protection of certain health information. he Security Standards for the Protection of Electronic Protected Health Information (the Security Rule) establish a national set of security standards for protecting certain health information that is held or transferred in electronic form.

Even if QUARTZ Program is HIPAA compliant, any data handled by organizations outside the US like QUARTZ Program do not come under the purview of HIPAA.