Health Innovation Hub Ireland

THE GENERAL DATA PROTECTION REGULATION (GDPR)

After reading this fact sheet you should:

- Have an introductory knowledge of GDPR and
- Understand some of the GDPR impacts and considerations for medical device innovators.
- Have links to related resources.

As a medical device innovator, it's important you are aware of GDPR and that non-compliance carries serious penalties. Therefore you should dedicate time and resources to it, as appropriate.

What is GDPR?

The General Data Protection Regulation (GDPR) **Regulation (EU) 2016/679** became effective on 25 May 2018, superseding the previous EU privacy law EU Directive 95/46/EC. Its main objectives are to strengthen the rights of individuals, and to streamline the rules and regulations, with respect to the protection, processing and movement of Personal Data by other people and by organisations across the EU. In particular, Article 8(1) states that "everyone has a right to the protection of personal data concerning him or her". Data subjects have the right to be forgotten, rights around the portability of their data and the right to object to their data being subjected to automated decision making. GDPR does not apply to anonymous data or data related to deceased persons.

GDPR is extra-territorial and applies to any organisation that collects or processes personal data of individuals inside the EU, regardless of where such organisations are located. It covers EU residents and non-residents residing in or visiting the EU while they are in the EU and makes provision for fines of up to €20 million or 4% of global turnover for serious breaches of the law. GDPR is not specific to medical devices but is the legal framework in the EU for the processing of health data, which the GDPR defines as any personal data relating to the physical or mental health of an individual, including any health care service which may reveal information about the person's health status. Therefore GDPR imposes a burden on innovators in medical devices and/or medical software that deals with patient data.

What are the fundamentals of GPRR?

The Irish Government's Citizen's Information website gives a concise **GDPR overview** in respect of:

- Data protection language.
- Special categories of data and limits on processing.
- The **obligations of organisations** with respect to the controlling and processing personal data.

You should also become familiar with data protection principles. i.e., personal data should be:

- Processed lawfully, fairly and transparently.
- Collected for specified, explicit and legitimate purposes and be processed in a compatible manner.
- Accurate, relevant and limited to what is necessary for purpose.
- Kept up-to-date, and inaccurate data should be rectified without delay.
- Securely stored and protected against unlawful processing and accidental loss, destruction or damage.
- Stored for no longer than necessary for the purpose for which it is required, especially where personal data is in a form that identifies the data subject. (Exemptions may apply).

A good starting point for adopting GDPR principles is simply to adopt the approach of 'Privacy by Design', i.e., think about data protection from the outset, viewing it holistically and implementing privacy by design in all processes.

Does GDPR apply to me?

Innovators working to develop and commercialise a medical device will need to comply with the EU medical device regulations **EU MDR 2017/745** or **EU IVDR 2017/746** irrespective of GDPR. However, if your medical device or medical device software collects personal data, then GDPR compliance is a prerequisite for compliance with MDR or IVDR. Building an MDR/IVDR compliant application requires a suitable Quality Management System and GDPR-compliant technology. **HERE** is a useful resource: "Ultimate Guide to ISO 13485 Quality Management System (QMS) for Medical Devices".

What are the data technology considerations for GDPR?

Since you are legally responsible for the lawful and safe processing, management and storage of the data you must implement various physical, technical and administrative requirements for GDPR. Physical requirements include facility protection, firewalls, virtual machine security, and system administration. Technical requirements are the most challenging and include data encryption, authorisation and access control, consent tracking, and immutable audit logs. Lastly, administrative requirements include privacy policies, terms and conditions, and GDPR Data Privacy Impact Assessment, and risk impact assessment.

What about health, genetic or biometric data?

This data is a 'special category of personal data' under GDPR, meaning it is considered particularly sensitive as its misuse poses greater risks to data subjects. As an innovator, if you are developing a DigiHealth product you should take care if processing this category of data. Appropriate data protection technical measures including pseudonymisation and encryption.

Who manages the data?

The data controller determines the purposes, conditions and means of processing of personal data. You need to identify the data controller or joint data controllers for your medical device. The data controller is responsible for ensuring compliance with the principles of GDPR. A **Data Protection Impact Assessment** (DPIA) is used to identity and mitigate against data protection risks. DPIAs are mandatory for new high risk processing projects. A data processor may process data on behalf on the data controller.

Do I need to obtain patient consent?

To comply with the lawful processing of special category data DigiHealth companies might typically rely on obtaining 'explicit consent' from the customers or users of their device or App. But be aware that 'consent' is interpreted in a specific way for the purposes of the GDPR. i.e., it must be given by a clear affirmative act, be freely given, and be specific, informed, and unambiguous.

Privacy notices must provide clear, intelligible and concise information to individuals on what personal data is collected, and how that data is processed. When dealing with vulnerable adults or children, information about data processing must be especially transparent.

How does GDPR apply to clinical investigations?

The EU Commission states that "... it is the obligation of the data controller to implement the appropriate technical and organisational measures to ensure and be able to demonstrate that the personal data are processed in accordance with the data protection rules". Recently, the EU Commission published a **Q&A document** on the interplay between the Clinical Trials Regulation and GDPR.

Are there any Ireland-specific regulations?

From an Ireland perspective, please review the following:

- **Data Protection Bill 2018** giving further effect to **GDPR Regulation (EU) 2016/679**.
- The **Health Research Regulations 2018** govern the use of personal data for health research purposes, in which mandatory **suitable and specific measures are outlined**, ensuring that health research in Ireland is conducted using best practice principles of information governance in line with new GDPR requirements.
- For more information on consent declarations in health research, visit the **Health Research Consent Declaration Committee**.

Health Innovation Hub Ireland
info@hih.ie
www.hih.ie

HIHI (UCC)
Western Gateway Building
University College Cork
Cork, Ireland
+353 (0)21 420 5560

HIHI (TCD)
H&H Building
St James' Hospital
Dublin 8, Ireland
+353 (0)1 896 2573

HIHI (NUI Galway)
Lambe Institute
National University of Ireland
Galway, Ireland
+353 (0)91 492 072

HIHI (MTU)
CREATE Building
Munster Technological University
Cork, Ireland
+353 (0)21 432 6758