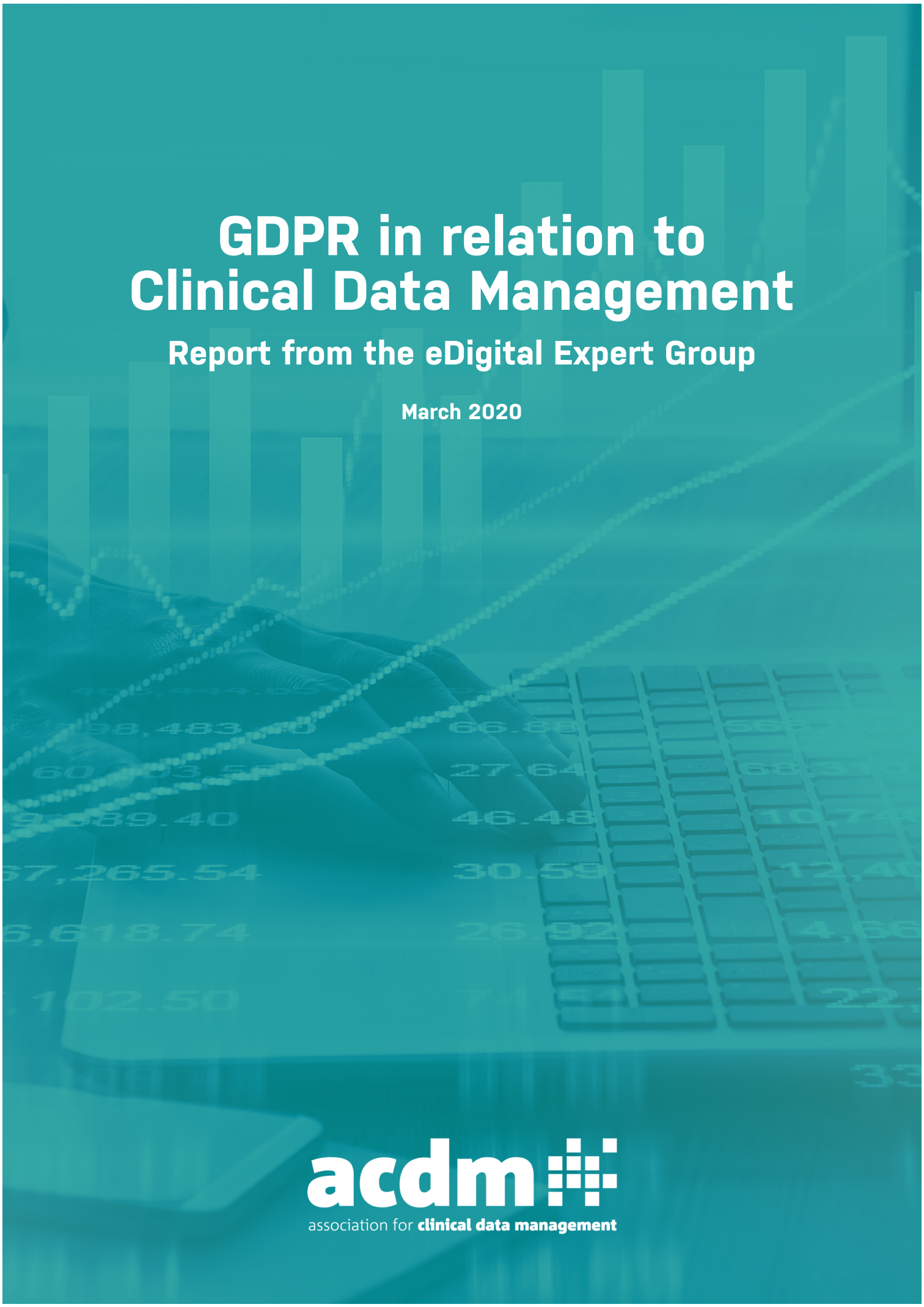
GDPR in relation to Clinical Data Management

Report from the eDigital Expert Group

March 2020



acdm
association for clinical data management

Summary report of the questions raised and the answers provided during the eDigital team's Q&A on the issue of GDPR in relation to clinical data management.

What data should participants have access to?

In some trials, patients may be asked to provide data using wearables, to fill in information on the web or use an app over a mobile device. In these circumstances the patient may have access to their data for engagement purposes. More commonly, the subject is not allowed to see the data they have previously provided to prevent bias, however access to this data may be provided at the end of the study.

The type of information being collected must be described and the patient must have provided informed consent. One of the rights outlined in GDPR is the "right to access" and, in respect to research, this should be provided if there aren't compelling reasons to prevent such access, such as risk of bias, as described above, or in the context of a blind trial.

What information should we collect from wearables?

The amount of information we can get from technology is vast, however the data that is chosen to be collected must be relevant to the study and the source dataset must be able to be transferred to the study investigator. For example, you should consider whether the source dataset for an accelerometer would be too large to share with the investigator.

How long should research data be kept?

During informed consent and before the start of the trial, data subjects should be informed how long the data will be kept and the location. Even after this period has elapsed, you may be able to rely on other legal bases to retain the data, such as for archiving purposes in the public interest; scientific or historical research purposes. The duration that data may be kept for could depend on national law and concrete circumstances. In certain cases, informing the patients of the continued storage (above the period communicated in the consent form) may be required.

Can the study data be used again?

There are different types of legal reasons for using already collected data. One well known reason is "patient consent" but another is the "legitimate interest of the sponsor". This can vary across different countries, for example Germany will only accept patient consent whereas other countries allow sponsors and sites to use 'legitimate interest of the sponsor' as legal basis (article 6 GDPR) and, in these countries, it is not required to ask the patient to reconsent. A core theme in GDPR is transparency, therefore data subjects must be informed that their data may be reused, if this was not done during the consent process then all patients will typically need to be informed of the change.

During an oncology registry study in Germany, patients were consented to a 5 year follow up period. At a later stage the sponsor, wanted to invite the patients back for a second study, however during years 6-10, the sites informed them that the patient had died. Can we collect the knowledge of patient death in study data?

GDPR only protects data subjects of natural living people, therefore this data can be collected. However, some national laws may provide some obligations regarding processing personal data of deceased persons (e.g. France).

How long can you save data that has been collected during the pre-screening process?

If the data controller is the sponsor you can either consider that pre-screening is part of the trial itself and then you can include it in the total study data or you could consider that the pre-screening is separate to the clinical trial and therefore it should follow a different process. However, you can also determine that the site is the data controller for the pre-screening, and that is a separate process from the clinical study.

There is discussion ongoing in the EU, whether sites are controllers or processors in Clinical Trials. Some countries consider sites are controllers, whereas other countries consider them to be processors.

Following a data deletion request, what should you delete?

Research data of consented subjects cannot be deleted, which is vital to protect from unscrupulous researchers that could use this as an excuse to remove less desirable responses from their dataset before submission. A data subject can stop providing additional data.

When there are valid use cases where data can be deleted it can never be deleted from the audit trail. It must always be possible to recreate the events of the trial afterwards.

What is the difference between pseudonymisation and anonymisation?

Pseudonymisation describes the process of replacing direct and indirect identifiers (like last name, date of birth, social security number, postal address) by codes or by blank: the goal is to make it impossible to re-identify a natural person without the right “key”. E.g. In the case that you remove the patient’s name and replace it with an identification number. There is ability to still link it back to the patient if you have the reference sheet linking the patient name and the identification number. Whereas, anonymisation is where all identifying data is permanently removed, and you can prove that it is impossible to re-identify the natural person.

If you have any questions please feel free to contact ACDM on admin@acdmglobal.org.