Challenges in identifying Data Controllers and Legal Bases and the developing role of hospitals in relation to research and data governance

Gillian Vale, 25 May 2021

It is now three years since the General Data Protection Regulations 2018 took effect. These years have represented intense real-time, on the job grappling with the legislation and attempting to interpret and apply it in all its intricacies in the area of research.

Following attendance at a training session hosted by CMG Training on the 18 May 2021 (presenter – Ms. Mary Kirwan, Barrister-at-law, and Legal Advisor to the Beaumont Hospital Ethics (Medical Research) Committee), I have drafted this piece to mark this point in time. The content stems from a case study attendees were asked to discuss with a view to attempting to identify the 'data controller' in a particular research scenario.

This piece highlights, as the title says, challenges in identifying data controllers and legal bases and the developing role of hospitals in relation to research and data governance.

1. Data Controllers…..

What the law says:

Data controller(s) and Data Processor(s) are 'natural persons' i.e. can be individuals or organisations

-v- the interpretation:

The Data Protection Commission / Department of Health / Health Research Consent Declaration Committee all place the emphasis on data controllers and data processors as organisations i.e. the 'organisational' data controller and the 'organisational' data processor (- See Trinity College Roundtable, 21.4.21 and Masterclass, 28.4.21)

Exception: A general practitioner who is a sole practitioner or an individual consultant in private practice

-v- institutional policies

Certain universities are reported to have local policies and practices in place which state that *their* organisation must always be named as data controller

Internal documentation from the HSE REC Reform Working Group tends to emphasise data controllers as organisations.

-v- reality for hospital sites

Irrespective of whether the university names itself as the data controller, the hospital in its role as 'data controller' of the personal data processed for the provision of healthcare is always implicitly / explicitly involved.

The hospital will always be the data controller for the personal data processed for the provision of healthcare.

The hospital may be the data controller for the personal data processed for the purposes of health research.

In respect of a particular health research project, the hospital may be a joint data-controller with the university.

Alternatively, it may be a data-processor 'processing data for the purposes of health research' on behalf of the university.

Alternatively, it may be a 'data controller' for one part of the health research, while the university is the 'data controller' for another part.

The fact the university states that the key to re-identify individual data subjects will remain at the hospital site does not mean that the university is not the data controller

If the health research project is designed by the university, they are controlling the purpose and means of processing i.e. the data controller

An area of significant difficulty for hospital sites is where data protection obligations start and stop and when hospital governance and oversight commences

A study is proposing to take place in a hospital and is being organised by a university.

The university has designed the study; they are controlling the purpose and means of processing, and are a data controller. They seek to conduct the study using personal data of 'data subjects' (patients) of a hospital with the permission of the hospital, and the support of hospital staff involved in treating the patients.

The university as the data controller must ensure it meets its obligations under GDPR, and the university employee may obtain advice from the university's data protection officer (DPO).

Obligations will include but are not limited to ensuring compliance with the principles of GDPR, upholding data subject rights, conducting a Data Protection Impact Assessment (DPIA), ensuring relevant contracts are in place, and ensuring information leaflets meet all the criteria for explicit

consent under the Health Research Regulations (HRRs) or that an exemption under the amendments to the HRRs applies or a consent declaration has been obtained.

Nonetheless, as the health research study will be taking place in the hospital, the hospital does need some governance and oversight processes.

How far these processes need to go, and how much the hospitals can take on trust that the research studies being conducted by universities are data-protection compliant is an area of difficulty.

The recent HSE Audit of Genuity Science Ireland (a commercial company conducting genomic research in multiple hospitals) suggests that hospitals should, at least going forward, check if study information leaflets / consent forms meet the minimum criteria for transparency under GDPR.

There is the implication that the hospital has a compliance-checking role when permitting research to take place on the premises. This is irrespective of who the stated 'data controller' is in respect of the research study.

By permitting a university or commercial organisation to conduct research in the hospital, the hospital is involved, and required to assume a level of responsibility from a governance perspective.

Them –or- Us

Many of the studies which do take place, irrespective of whether the hospital is the data controller or not, tend to direct the patient (data subjects) to the hospital data protection officer (dpo) to give effect to their rights – as opposed to the university or commercial company dpo.

There appears to be a reluctance on the part of university or commercial data controllers to take full responsibility for this aspect of data protection – and hence, a tacit understanding that the hospital has a role to play, albeit not being named as a data controller.

In the event of a fine, or prosecution or class action in the event of non-compliance with GDPR, the hospital is also likely to be named (as a data controller) given that the data subjects are patients of the hospital.

The difficulty in identifying who the data controllers and processors are, and what the hospital's role is becomes further compounded by the fact that if one fails to correctly name the hospital as either a data controller or processor, the chances are that one is not entering into a data processing agreement with the hospital.

Failure to put data processing agreements in place is itself a breach of GDPR.

The Legal Reality

"A very interesting case in terms of identifying the data controller is the Mount Carmel case. In the Matter of Mount Carmel Medical Group (South Dublin) Ltd.(in liquidation)[2015]IEHC450 considered the issue of who was data controller in respect of the company during a liquidation. The decision in

this case showed that the court will give limited weight to any contractual provision designating a particular party as data controller, and will instead focus on who, in fact, exercises control over the personal data concerned." (– Mary Kirwan, Barrister at Law)

2. Legal Bases…..

What the law says:

An article 6 legal basis is required to process personal data under GDPR.

Practical Difficulties

Not all legal bases are open to all organisations, for example, a public hospital is not permitted to use 'legitimate interest' as a legal basis, and there may be circumstances where it is not recommended that the hospital use 'consent' as a legal basis.

Similarly, a commercial organisation cannot use 'public interest' as a legal basis.

Identifying Data Controllers and their Legal Bases

Where there is one data controller and that data controller is a public hospital (e.g. Beaumont Hospital) the legal basis will likely be 'public interest'

Where there is one data controller and the data controller is a private hospital (e.g. Blackrock Clinic) the legal basis will likely be 'legitimate interest' in the conduct of research.

Where there is one data controller and that data controller is a public university (e.g. UCD) the legal basis will likely be 'public interest'

Where there is one data controller and that data controller is a private university (e.g. RCSI) the legal basis will likely be 'legitimate interest' in the conduct of research.

Where there is one data controller and that data controller is a charity (e.g. The Alpha One Foundation), the legal basis will likely be 'legitimate interest' in the conduct of research.

Informing the data subject

The data controller must inform the data subject (participant) of the legal basis for processing, usually via a Research Participant Information Leaflet.

Where there are multiple data controllers, each data controller must be identified and the legal basis each of these controllers is relying upon must be stated.

This is not easy to do, and far from easy for a health researcher to do.

Article 9 condition

What the law says:

When processing special category personal data, an article 9 legal condition is also required (in addition to an article 6 legal basis)

In practical terms:

In practical terms, this is a relatively easy, as all organisations and organisation types are permitted to use 'scientific research' as an article 9 condition.

Informing the participant

Data Subjects (participants) must be informed of the article 9 condition in the Research Participant Information Leaflet

3. Summary…..

Identifying which parties in a health research project are data controllers, joint data controllers and processors is challenging.

Identifying the Art 6 legal basis to rely on is particularly difficult when there are multiple data controllers all relying on different legal bases.

Irrespective of which organisation or individual is ostensibly named as the data controller, the hospital where the research is conducted is always involved and implicated by default, and an over-sight and governance role applies.

4. Epilogue…..

If you are reading this as an applicant to a research ethics committee, I hope this might cause pause for thought before:

- naming the data controller
- stating the Article 6 legal basis
- naming the data protection officer
- considering if contracts are required with the hospital

These considerations are not neutral ones, and have implications for you as the researcher, for the organisation you are studying with or working in, and for the hospital you wish to conduct the research in.

The unfortunate reality is that at least one of the research studies permitted to take place in the hospital will result in a fine, prosecution, or law suit.

In light of the ransomware attack on the HSE in May 2021, 'data breaches' including breaches which need to be reported to the Data Protection Commission are no longer a 'hypothetical' risk in the Data Protection Impact Assessment (DPIA).

Subject access requests where data subjects seek to access the personal data you hold on them, and requests from data subjects to exercise their rights will very likely increase over time.

Finally, remember that GDPR has been immensely challenging for the large-scale, multi-national, commercial organisations with large legal departments, but is equally as challenging and complex for the single health researcher.

If you don't understand it you are not alone!