RCVS Ethics Review Panel (ERP) Guidance on handling personal data in Clinical Veterinary Research

This guidance note aims to provide some useful background and pointers that will help you to develop your application(s) in relation to personal data and research. By necessity guidance in this area touches upon both legal and ethical issues associated with personal data use and its management in research. However, we present it as an aid to developing your research ethics application as opposed to providing legal advice on personal data use.

It is important to always distinguish between personal data and scientific data, and to note that it is the former that needs to be protected.

What is personal data?

In data protection legislation data is personal if:

1. It pertains to a living human person
2. The person could be identified from the data
3. The processing (use) of the data relates to the identifiable living person

Some examples pertaining to personal data in common veterinary research scenarios:

- Many clinically focused veterinary projects making use of clinical records retrospectively do not use personal data. For example, a pet focused clinical project in which the owner is not the subject might not use any personal data.
- Other veterinary clinical research projects do use personal data. Some examples include:
    - If data such as the owner's name and address are being used to contact owners for clinical follow-up.
    - If a project is using clinical records data and considers variables such as impact of owner finances on veterinary clinical decision making.
    - If the demography (gender, age, job title), professional activities or opinions of practice staff are being studied.
- Social science research aimed at developing our understanding of the interaction between animals and humans may intentionally or unintentionally collect personal data due to the nature of the research methods therefore a particularly careful consideration of the research and data protection methods is required.

There are many possibilities and therefore researchers must consider their research methods carefully.

Why is the proper handling of personal data important?

There are both legal and ethical reasons why proper handling of personal data is important.

From a legal perspective, the collection, use and storage of personal data is regulated under the Data Protection Act (2018) (DPA), which is the UK implementation of the EU General Data Protection Regulations (2018). The Information Commissioners Office (ICO) oversee personal data use in the UK, and where data protection rules are breached very significant fines can be imposed.

The DPA lays out seven principles regarding processing of personal data:

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation
- Accuracy

- Storage limitation
- Integrity and confidentiality (security)
- Accountability

From an ethical standpoint, public support for research depends upon researchers demonstrating high standards of morality and integrity in their work. Correct use, management and storage of personal data to comply with relevant legislation and protect research participants (i.e. humans who have consented to participate in the research, as opposed to animals which are better described as animal subjects) is an essential part of such morality and integrity. In considering an application, one of the areas on which the ERP focuses is how the use and storage of data is described in the research consent process

When can I work with personal data?

The DPA requires that processing of personal data has a 'lawful basis' (of which there are six). Those processing personal data should consider what lawful basis they have for doing so; the lawful basis used should be recorded. The lawful bases are listed and explained on the ICO website (https://ico.org.uk), but the most relevant ones in the veterinary research context are likely to be 'public task', and 'legitimate interest'. Applicants are encouraged to read the guidance and gain an understanding of these prior to completing their application. Researchers should note that ICO guidance states that often 'consent' is often *not* the ideal lawful basis for data processing for research. The ERP will consider proposed personal data use and will advise if we have ethical concerns (although applicants should not construe this as legal opinion).

If it is legal to use the data in the manner proposed, the ERP will also consider whether it believes it is ethical. In this context the ERP will look for a demonstration of informed consent relevant to the research context, its use and the data storage plan that suitably protects the participants (usually the animal owners). **Perhaps the most obvious example here is that data use statements buried deep in contracts or privacy notices or the use of data mandated as part of a clinical service agreement may not be considered appropriate in some contexts.**

Anonymisation, confidentiality and personal data

Collecting, storing and transmitting data in anonymised form is one way to protect participants. However, anonymisation is often more straightforward in principle than in practice and a few definitions are worth considering:

Truly anonymised data does not allow identification by any participant. Use of true anonymisation can be helpful in avoiding data protection issues (as by definition no personal data is collected). However, in many cases, such as use of small clinical records data sets, true anonymisation may not be feasible because the researchers will retain knowledge of aspects of cases that allow identification.

True anonymisation makes it impossible for participants to withdraw their data from the study and it is therefore important to warn participants in the information sheet if this is the case. Examples of this might be to collect all the weekly pooled urine samples in a clinic or anonymously collect survey results.

Linked anonymisation (aka **pseudonymisation**) is a process that replaces immediately identifiable information with a code. As such it can be particularly useful for protecting data when transferring datasets between researchers. It should be noted, however, that pseudonymised data remains identifiable by holders of the code key and consequently can remain personal data in many contexts. For social research using qualitative methods it is usually necessary for the raw research data to be transcribed into a written document, linked to the participant using a code, which is both anonymised and decontextualized such that the research participant cannot be identified. This form of

anonymisation can be carried out manually or by using dedicated software either during or after transcription. It is the responsibility of the researcher to ensure that the process has effectively obscured all identifying features. A brief UKRI guide to anonymisation techniques can be found here: https://ukdataservice.ac.uk/learning-hub/research-data-management/anonymisation/anonymising-quantitative-data/.

Regardless of the form of anonymisation, participant confidentiality is an important principle in research. Applications should therefore reassure participants that any personal data that may be needed for research purposes will be kept securely and confidentially. Indeed, researchers should pseudonymise research data as soon as practicable after collection.

One exception to the general rules around confidentiality, is that some studies carry a risk that participants may disclose an illegal activity that researchers would have a legal or professional obligation to report (e.g. abuse of animals, a breach of professional standards). When such a risk exists, participants should be made aware of what action the researchers are required to take prior to consent being given.

Data and research publications

It is expected that research results will be published in anonymised form in all but a tiny minority of contexts. Researchers should nevertheless consider the risk of triangulation (the possibility that several pieces of data taken together could allow the identification of individuals even when results are published with the intent that they are anonymous). Researchers should publish results in a form that prevents identification by triangulation, particularly when there is a risk of financial or other harm to owners of animals or other stakeholders through loss of confidentiality.

Some common veterinary situations in which there is a risk of triangulation include:

- Studies of a rare breed or species of animal that may only be kept by a small number of people.
- Large farms that cover an entire postcode area.
- Any sensitive demographic information.
- Studies looking at service delivery that might allow identification of practice staff.

The risk of triangulation can be reduced by reporting data in larger aggregate forms. One commonly used approach is to report in larger geographical areas (e.g. 4 letter post code or even county level rather than the full 7 letter postcodes).

Personal data transfers between parts of a research team

Data transfers inevitably carry the risk of data interception or loss. Identifiable research data should not be transferred. In some cases, linked anonymisation may provide sufficient protection, but when loss of data might carry significant implications for individuals full encryption is preferred.

In this context applicants should also consider the potential for personal data to be accessed via hacked email accounts.

In addition the applicants using international multicentre studies should check on the legality of any personal data exchange import or export. For example, in the context of international research, explicit consent is required to transfer personal data out of the EU.

Personal and scientific data storage

Researchers should take adequate precautions to protect research data during a project. However, they should also retain research data for a sufficient length of time after publication to allow for review of anonymised primary data by appropriately interested parties if necessary.

Prior to publication, personal data may be more likely to be directly identifiable and consequently should be protected by security measures such as locked cabinets for physical copies and encryption and passwords for electronic copies. Retaining data within commercially maintained IT infrastructure (e.g. institutional IT systems) may also add to the protection via backups and security features such as firewalls.

Post-publication anonymisation of personal data adds another layer of protection and allows for longer-term storage of such data at a lower level of risk. In principle it may be possible to store anonymised data and scientific data indefinitely.

Throughout the period of data collection, use and storage, it is helpful to have a single individual in each centre who takes overall responsibility for monitoring data processing and ensuring that it is in keeping with both legal and ethical stipulations. In many cases this individual will be the primary investigator and/or the chief investigator in each centre, but it is helpful to explicitly stipulate the responsible person within an application.

RCVS ERP reviews and personal data

As alluded to above the RCVS ERP, as part of the review process, will provide advice on ethical issues around the proposed handling and storage of personal data for a project. As part of this, if it has concerns about legal aspects of data handling that will be highlighted, but the ERP does not provide formal legal advice about adherence to data protection or GDPR compliance. That responsibility lies with the researchers who, when necessary, should seek clarification via the Information Commissioners Office or the Institutional Data Controller, or a solicitor with appropriate training and experience when necessary.

Resources

- Information Commissioners Office website - https://ico.org.uk
- Draft guidance on the research provisions within the UK GDPR and the DPA 2018 - (https://ico.org.uk/media/about-the-ico/consultations/4019614/research-provisions-draft-consultation-202202.pdf)
- UK Data Protection (2018) - https://www.gov.uk/data-protection
- RCVS Code of Professional Conduct - https://www.rcvs.org.uk/setting-standards/advice-and-guidance/code-of-professional-conduct-for-veterinary-surgeons/