UGANDA

Cross-Border Sharing of Data

This section reviews the rules as required by data protection law in the cross-border sharing of personal data. The rules on the cross-border sharing of personal data under data protection law do not exist in a vacuum, and therefore other important information that must be followed when sharing personal data is discussed. This information, however, is comprehensive as it relates to the cross-border sharing of personal data.

The relevant national health research regulations as they relate to the cross-border sharing of personal data are reviewed. These national health research regulations set out the required legal and ethical conditions that must be met when processing personal data for research. Applicable national legal and ethical documents are listed, but the discussion only specifies the requirements as they relate to the cross-border sharing of personal data for research. The guide does not treat the legal and ethical requirements generally required for research, and therefore users of this guide must consult with these documents to ascertain these requirements and to ensure that they are met.

An overview of the data protection law is provided. This includes what data the law applies to, the categories of data, the key individuals in the DPPA, the key principles required to be met in the processing of personal data, and the rights of data subjects. This is an overview only to help users to understand *some* of the requirements of the DPPA and to begin to assist users in navigating it. It is not comprehensive, and users of the DPPA must consult it to understand all relevant and applicable requirements to be met, and to understand any exceptions that may be in place for research. This is necessary as all these requirements must be met in the processing of personal data for research, in addition to the requirements on cross-border sharing of data.

The section provides users with a comprehensive description of the requirements to be met in the cross-border sharing of personal data for research. It sets out all the necessary conditions that must be met to legally share data across borders for research.

In countries where no data protection law is in force, the necessary national legal and ethical requirements, as they relate to the cross-border sharing of data, are presented.

The cross-border sharing of personal data is governed by several laws and regulations, which must be carefully considered and complied with before researchers share data for research purposes. In Uganda, the Data Protection and Privacy Act is in place. It is a general data protection law that applies to the processing (i.e., use) of personal data in all sectors. While it is not a statute introduced

specifically to regulate research, it applies to research that involves the processing of personal data. It must be complied with when transferring personal data for research purposes.

Health Research Regulations Involving Human Participants and Cross-Border Data Sharing

In addition to the national laws listed below, several international treaties and conventions have been signed. Of importance in this domain is the African Union Convention on Cyber Security and Personal Data Protection ('the Malabo Convention'). Uganda has not ratified the Malabo Convention.

The relevant national health legislation and guidelines are:

- Guidelines on Good Clinical Practice in the Conduct of Clinical Trials Involving Human Participants, 2019
- National Guidelines for Research Involving Humans as Research Participants, 2014
- National ICT Policy, 2014
- Access to Information Act
- Public Health Act
- Uganda Health Research Organization Act

These laws, policies and guidelines set out the legal and ethical requirements that must be met for the conduct of research in Uganda and must be considered when effecting cross-border transfer of personal data. Furthermore, specifically for the cross-border sharing of data, a Research Ethics Committee must approve any cross-border data sharing, and there must be a local Principal Investigator and a MTA.

Data Protection and Privacy Act

In addition to these legal and ethical requirements, the Data Protection and Privacy Act applies to the processing of all personal data, but unlike most data protection regulations there are no special provisions in place for scientific research. The conditions set out in the Act must all be met for

research. In addition, extra conditions must be met prior to the transfer of personal data across borders.

Some of the techno-legal terms used in this Act are discussed/defined below. This is not a thorough assessment of the Act as it applies to research, but rather an overview of some of the key terms and conditions that must be met in the processing of personal data for research.

The Main Actors Defined in the Data Protection and Privacy Act

	Legal definition	**Layman explanation**
Data subject	An individual from whom or in respect of whom personal information has been requested, collected, collated, processed or stored.	The person to whom the data relates.
Data controller	A person who alone, jointly with other persons or in common with other persons, or as a statutory duty, determines the purposes for and the manner in which personal data is processed or is to be processed.	The person who decides what the data will be used for in research. Legal responsibility falls on the PI *and* on the research institution (as employer).
Data processor	A person other than an employee of the data controller who processes the data on behalf of the data controller.	Someone who is not directly employed by the data controller but who processes personal data under the direction of the data controller. They may be a consultant, for example.

Authority	The National Information Technology Authority.	The independent body established to monitor and enforce compliance with the law.
Data Protection Officer	Not defined in the Act, but provided for in the Act.	An individual in an organisation who is appointed to advise and to promote compliance with the law.
Recipient	A person to whom data is disclosed including an employee or agent of the data controller or the data processor to whom data is disclosed in the course of processing the data for the data controller. But this does not include a person to whom disclosure is made in respect of a particular inquiry pursuant to an enactment.	
Data collector	A person who collects personal data.	
Third party	A person other than the data subject, the data collector, data controller, or any data processor or other person authorised to process data for the data controller or data processor.	

Categories of Data Listed in the Data Protection and Privacy Act

	Legal definition	**Layman explanation**

Personal data	Information about a person from which the person can be identified, which is recorded in any form and includes data that relates to: (a) the nationality, age or marital status of the person; (b) the education level or occupation of the person; (c) an identification number, symbol or other particulars assigned to a person; (d) identity data; or (e) other information which is in the possession of, or is likely to come into the possession of, the data controller and includes an expression of opinion about the individual.	Data/information about a particular person that can identify him or her.
Special personal data	Not defined. However, the Act provides that special personal data relates to religious or philosophical beliefs, political opinion, sexual life, financial information, health status, or the medical records of an individual	Personal data about a particular person that is particularly sensitive, such as health data and genetic data, and which receives additional legal protection.

Generally, data protection law applies only to personal data. This is data that refers to an identified or identifiable person. For data that does not come under the definition of personal data, data protection law does not apply. The Data Protection and Privacy Act, like many other data protection laws, applies specifically to the processing of "personal data". The Act defines personal data as "information about a person from which the person can be identified". Therefore, if the data is not personally identifiable, such as where it has been anonymised, it would not fall under the application of the Act. The terms 'de-identified' or 'anonymised' are not used in the Act.

To determine whether data to be shared is anonymised, it is important to make an assessment, which can be challenging. There is no guidance from the Authority on this point, but the data controller may wish to follow the guidance set out to be followed under the GDPR on how to make an assessment to determine whether data has been anonymised – including anonymisation techniques.

The test for anonymisation is always objective, but it can be interpreted in two ways: context-specific (relative approach) or context-agnostic (absolute approach).

Accordingly, the test for determining whether data is anonymised can be approached in two ways:

1. **Context-Agnostic Test**: Is there anyone in the world who can identify the data subject from the data? This test assesses whether any individual, regardless of context, could identify the data subject.
2. **Context-Specific Test**: Can a specific holder of the data identify the data subject from the data? This test evaluates whether the specific data recipient, given their context and resources, can identify the data subject.

The choice of approach affects the treatment of pseudonymised data. For example:

1. **Context-Agnostic Test**: If Data Controller A sends pseudonymised data to Data Controller B (with A retaining the means to identify individuals), the dataset is not considered anonymised.
2. **Context-Specific Test**: If Data Controller A sends pseudonymised data to Data Controller B, the dataset *might* be considered anonymised in the hands of Controller B. However, a test is necessary to determine if the dataset is indeed anonymised for Data Controller B.

The first test would mean that if Data Controller A sends pseudonymised data (i.e., Data Controller A has the necessary information to identify the people in the dataset) to Controller B, the dataset would not be anonymous.

The second test would mean that if Data Controller A sends pseudonymised data (i.e., Data Controller A has the necessary information to identify the people in the dataset) to Controller B, the dataset *may* be anonymous in the hands of Data Controller B. A test would be needed to determine whether the dataset is anonymous in the hands of Data Controller B.

In the absence of direction from the Commissioner on a test, the data controller will have to decide. In making this decision, general points may be worth bearing in mind (many of which come from guidance related to anonymisation under the GDPR):

- An assessment must be made on a case-by-case basis, considering the particular context.
- The anonymisation must be irreversible.
- The assessment is made on the current state of the art. As technology progresses, data that was once deemed to be anonymous may become personal data and therefore fall under data protection regulations.
- Consider all means of identification that could be used by a person, for example, available datasets.
- Consider objective factors that are *reasonably likely* to be used, such as technology, resources and time, to identify.
- One could follow the GDPR test which states that if an individual cannot be singled out, or identifiers cannot be linked to make a person identifiable, or it is impossible to infer a link between two pieces of information in a dataset, then the data is anonymous.
- Genetic data is considered sensitive personal data. It not only falls under the Data Protection Act but also has a higher level of protection.
- There is ongoing debate about whether genomic datasets can ever be rendered truly anonymised, in particular as genetic data is an identifier. In considering whether a genomic dataset can be considered anonymised, context matters – the objective factors associated with the data.

Key Principles That Must be Met in Terms of the Data Protection and Privacy Act

1. *Accountability: Be accountable to the data subject for data collected, processed, held or used.* The data controller, data processor or data collector are responsible for, and must be able to demonstrate compliance with, the principles mentioned above. Keep a record of data processing activities, measures introduced to protect the data, and any risk assessments made. This can be used to demonstrate compliance in the event of a breach.
2. *Collect and process data fairly and lawfully:* Personal data must be processed lawfully, fairly, and transparently in relation to the data subject. Lawful means that there must be a legal basis for the processing of the personal data as set out in law.
3. *Data minimisation: Collect, process or hold adequate, relevant and not excessive or unnecessary personal data.* Only the data that is necessary for the specific purpose should be collected and processed. It is essential that only the minimal amount of data that is required to achieve the objectives of the data processing is used.
4. *Storage limitation: The data collector, data processor or data controller or any person who collects, processes, holds or uses personal data should retain it for the period authorised or for which it is required.* Personal data should be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed. Once the objective of the processing has been achieved, the data should be deleted. Data that is rendered anonymous does not fall under data protection law. However, to anonymise the data, there must still be a lawful basis to do so.
5. *Data quality: Ensure quality of information collected, processed, used or held:* Personal data must be accurate and, where necessary, kept up to date. Processes should be in place to ensure that all personal data collected is accurate.
6. *Openness: Ensure transparency and participation of the data subject in the collection, processing, use and holding of personal data:* Personal data must be processed lawfully, fairly, and transparently in relation to the data subject. Lawful means that there must be a legal basis for the processing of the personal data as set on in the Act. The processing of sensitive personal data is generally permitted unless it falls within one of the grounds as set out in the Act.

7. *Observe security safeguards in respect of the data:* Personal data should be processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures. Both organisational and technical measures must be put in place to secure the data.

Data Subject Rights Under the Data Protection and Privacy Act

Data subjects have rights that the data controller must protect. These rights are the:

1. *Right to access personal information:* A data subject who provides proof of identity may request a data controller to confirm whether the data controller holds personal data about the data subject, give a description of the personal data which is held by the data controller, and provide the identity of a third party or a category of a third party who has or has had access to information.
2. *Right to prevent processing of personal data:* A data subject must at any time by notice in writing to a data controller or data processor, require the data controller or data processor to stop processing personal data which causes or is likely to cause unwarranted substantial damage or distress to the data subject. In addition, a data controller must within 14 days after receipt of a notice inform the data subject in writing that the data controller has complied or intends to comply with the notice of the data subject, or give the reasons for non-compliance.
3. *Right to prevent processing of data for direct marketing:* A data subject may by notice in writing to a data controller, require the data controller to stop processing his or her personal data for purposes of direct marketing. In addition, a data controller must within 14 days after receipt of notice inform the data subject in writing that the data controller has complied or intends to comply with the notice of the data subject, or give the reasons for non-compliance.
4. *Rights in relation to automated decision-making:* A data subject may by notice in writing to a data controller require the data controller to ensure that any decision taken by or on behalf of the data controller which significantly affects that data subject is not based solely on the processing by automatic means of personal data in respect of the data subject.

5. *Right to rectification, blocking, erasure and destruction of personal data:* Where the Authority is satisfied about the complaint of a data subject that personal data on that data subject is inaccurate, the Authority may order the data controller to rectify, update, block, erase or destroy the data.

Cross-Border Data Sharing

Each of the provisions applies to any research that uses personal data. Data protection law also has additional provisions that must be met when personal data is to be transferred outside the country. These additional provisions are in place to ensure that data subjects continue to be protected once the data leaves the country.

While cross-border sharing is not defined in data protection law, the laws on cross-border data sharing clearly apply to data sent to a data controller in another country. It *could* also include when a researcher outside of the country accesses the personal data in the country. It *could* also include putting data onto a cloud where the server is not hosted in the country. Whether it does or not is not yet settled law.

In addition, there must be a ground under which transfer can occur. In terms of the Data Protection and Privacy Act, the legal bases for transferring personal (including health) data outside Uganda are:

1. The country in which the data is processed or stored has adequate measures in place for the protection of personal data that are at least equivalent to the protection provided for by the Act; or
2. The data subject has consented.