- Researchers at CAPHRI are required to design and conduct their research that deals with sensitive personal (medical) information in a way that privacy is respected.

Respecting privacy

European, Dutch and local laws, regulations and guidelines share a commitment to the protection of research subjects' privacy and ask of researchers that they produce and handle personal data carefully, refrain from sharing it beyond the research team and store and retain the data safely. Simultaneously, norms prescribing responsible research invite researchers to share data to allow reproduction and verification, and to store data for extended periods, to allow reanalysis or reuse.

Maastricht University's Data Management Code of Conduct attempts to operationalize both goals by making explicit how long you need to store data and where, whose property research data is and who can be granted access under which conditions to what. As a general rule, retain your data 10 years after the last publication and store it safely on UM servers. Researchers are free to grant other researchers access to their data, provided this does not breach other contractual obligations. Read the full text here. Practically, this means that members of the research team need to live up to a series of requirements.

Responsibilities

All researchers (including students and supporting staff)

Stimulate awareness among peers and research assistants;

Remain vigilant.

Project leaders

Document relevant decisions made regarding sensitive data (click for an example here);

Ensure compliance to these requirements from peers and research assistants;

Remain vigilant.

Vigilance

Never share access to accounts (UM or MUMC+), not to new peers or students, etc.;

Never leave your computer unlocked when leaving your office (locking your computer can be done by pressing 'windows button-L');

At the end of the day, put all sensitive info in secure storage;

Store all data on UM servers. Do not use local drives, flash drives, etc.

Permissions

Non-sensitive/anonymous data can be used without any restriction or permissions. Privacy is not a serious concern in this situation. Examples include statistical data from the CBS or number of patients who visited an institution or hospital. Anonymised data is considered anonymous only when identification of a person requires application of unreasonable means or disproportionate time and effort. Anonymous data, however, can be confidential because of agreements in the context of data collection, research prior to filing a patent or for (other) competitive reasons. Data that contains personal information, data that is not completely anonymised or data that cannot be anonymised (e.g. qualitative research data) is always considered sensitive and need to be treated accordingly. Collecting personal (medical) data requires informed consent to use or collect data. If consent cannot in all fairness be required or achieved, contact the METC or non-WMO IRB .

Handling

If possible, de-identify data during collection or directly after collection;

Collect only the variables required to answer your research question;

Store and process data always on UM/MUMC+ servers. Use data encryption when working outside the network. For info on encryption, see below.

Data incidents (data loss, hacks, etc.) need to be reported to the Caphri Quality Committee;

Storing and transporting data

Retain your data in accordance with Maastricht University Data Management Guidelines;

Storage and transport	*Cabinet*	*Digital*	*Email*	*Encrypted transport on mobile device*	*Cloud*
Non-sensitive data	No restrictions	No restrictions	No restrictions	No restrictions	Only ICTS offered and approved cloud services
Sensitive	Locked cabinet in a locked room	In a secured project directory, only accessible to the research team	Not allowed. Exceptions can be made for encrypted data, if project leader provides written permission	Only allowed when strictly required and data is encrypted.	Only ICTS offered and approved cloud services

Encryption

To encrypt sensitive data, we advise the open source platform 7zip. Use 265-AES encryption and a long password (recommendation of 12 characters or more). Do not send encrypted files and passwords using the same medium.

Online instructions for how to encrypte using 7zip, can be found here.

I declare that I have read the rules of privacy, data storage and handling, and I promise that I will act according to these rules.

Name: Place: Date: