Amsterdam Public Health

Amsterdam UMC University Medical Centers | VU Vrije Universiteit Amsterdam | University of Amsterdam

Privacy	Compliance, Training & Supervision - Compliance	
	VERSION	3.0

Aim
To provide a structured overview of how to handle and protect privacy sensitive data against unauthorized access, theft, and loss.

Requirements
To structurally follow the instructions described in this guideline.

Documentation
Document all important decisions made while following the instructions in this guideline.

Responsibilities
Executing researcher:

- To make sure all aspects of this guideline are considered regarding privacy sensitive data;
- To make sure all persons who have access to the privacy sensitive data sign or have signed a privacy statement;
- To document important decisions made regarding privacy sensitive data;
- Perform checks on the implementation of the security measures in this guideline;
- To make sure the research assistant(s) stick(s) to the Code of conduct for medical research;
- Be alert!

Project leaders:

- To make sure the executing researcher sticks to the Code of conduct for medical research;
- To make sure all aspects of this guideline are considered regarding privacy sensitive data;
- To sign the confidentiality agreement;
- To make sure a list is set up including all persons who (will) have access to the privacy sensitive data (see under Download for Dutch version and English version). Interns and others that are not fully employed by Amsterdam UMC have to sign the confidentiality agreement (click here; also see here).
- To register study details to the Centraal meldpunt gegevensverwerking of your organisation (VUmc: follow this link; AMC: follow this link; VU: follow this link)
- Check periodically if the access rights of the study team members are still necessary. Acces to e.g. network storage, data capturing systems sharing platforms (sharepoint, research cloud, Castor). This check must be documented.
- Be alert!

Research assistant:

- To sign the associated confidentiality agreement;
- To follow the instructions regarding handling privacy sensitive data in this guideline;
- Be alert!

How To
This guideline must be used as a guidance to correctly handle and protect privacy sensitive data. The most important aspect to note is this: when you are uncertain about aspects regarding privacy sensitive data it is important to contact the Quality Officer of APH or the privacy officer of your organisation!

Privacy statement:

Amsterdam Public Health

Amsterdam UMC University Medical Centers | VU Vrije Universiteit Amsterdam | University of Amsterdam

Handling privacy sensitive data daily

- Never share access to accounts (your VUmc account), not to a new colleague, not to a student, etc.;
- When leaving the office during the day: lock your computer screen, even if you leave for a few moments; Working @Home always lock your computer when leaving the room
- When leaving the office at the end of the day: clean your desk and put everything in a secure and locked storage;
- Store all data on the project file on the network. Do not use the C-drive or USB storage;
- Be alert!
- Help your colleagues to be alert: address them when sensitive information is unintentionally accessible.

When is permission needed for the use of data?
Anonymous data can be used without any restriction. Examples of anonymous data are statistical data from the Centraal Bureau voor de Statistiek or number of patients who visited a hospital. Anonymous data is data which can only lead to identification of the natural person after application of unreasonable means or disproportionate time and effort. Always ask for an assessment of the anonymity of your data from the privacy officer
Warning: anonymous data can be confidential because of agreements, research data prior to patent filing or competitive reasons.

The main principle about personal data is to ask for informed consent to use or collect data. If the request for consent cannot in all fairness be required, for example because this would cost a disproportionate amount of effort, data can under certain conditions be used for research without consent. Contacting the privacy officer or send a non-WMO proposal to the METc is obligatory if you estimate that informed consent cannot be obtained.
In general, the GDPR/AVG means that:

- It has to be proven that a research project complies with GDPR. This means you should document very well what you do and why. This documentation has to be available during and after finishing the project.
- Study subject have to be fully informed (see informed consent).
- Study subjects obtain new rights (for information: more transparency with regard to how and where data are handled; to withdrawal; to be forgotten; restricted to data that were not processed for scientific publications yet; to complain to the Privacy Officer or the Dutch Data Protection Authority (Autoriteit Persoonsgegevens).
- Written data protection agreements are needed for handling (f.i. sharing, collecting, saving) data by third parties.
- The use of genetic data has to comply to more strict regulations
- Every project (that collects privacy sensitive data) needs to conduct a Data Protection Impact Assessment (DPIA)

Handling data

- Make sure to de-identify the data during collection or directly after collection. This can be done by removing names, addresses, telephone numbers and IP addresses from e.g. datasets, transcripts and fieldnotes;
- Make sure to only process coded data (data that cannot be traced back to the individual person without the use of a key file);

- Collect only the variables you really need to answer your research question. Remove variables which you do not need to answer the specific research question in the data set used for analysis. This reduces the chances on identification of the individual person;
- To reduce identification risks: aggregate and substitute variables where possible. For instance change birth data into age ranges, reduce the numbers in postal codes, use BMI instead of body mass and length;
- Store and process data always on the network drives of the organisation. Use data encryption when working outside the network . See for instructions encryption, below the table Classification data for storage and transport;
- Never use email or open internet connections to transport identifying data including video and sound recordings, such as wetransfer, FTP (see also table Classification data for storage and transport).

Obligatory incident reporting
All incidents with privacy sensitive data must be reported to the privacy officer of your organisation without any delay. If a supervisor is not available for guidance, do not wait with reporting! Data breaches must be reported by the responsible organization to the data protection authorities within 72 hours after discovery of the breach. Reporting to the authorities only after advise of the data protection officer(s)

- VUmc privacy officer; privacy@vumc.nl
- VUmc intranet: meldknop Privacy Incidenten intranet (Meld Incident Storing Klacht)
- VU: itvo.ucit@vu.nl or socc@vu.nl
- AMC: click here

Examples of incidents (a “datalek”) are:

- Loss or theft of data carriers like USB sticks, portable drives laptops, tablets and data on paper;
- Hacking of databases, websites, computer systems;
- Wrongly sent e-mail or letter with personal data;
- Personal data that were destroyed mistakenly;
- Viewing the patient file of a family member or acquaintance;
- Sharing a file or document containing more personal data than necessary with a colleague.
- The Data protection authority has the power to impose fines up to €20.000.000 for not reported incidents!

Outsourcing: the use of third party services to store, transport, collect or process data
Examples of services: web based questionnaires, scan services, transcribing records, polling agency, webhosting, cloud storage etc.

- Third party services may only be used after written agreements are made about:
    - Secrecy,
    - Security arrangements, technical maintenance,
    - Handling incidents,
    - Destruction of data after termination.
- Only use services approved by the organisation.

Jurists of the team at IXA or Legal Research Support can help you drawing up agreements

Storage and Transport of data.
The storage of (privacy) sensitive and confidential information must be secure. The transportation of privacy sensitive data is only allowed when strictly necessary and with appropriate safety measures. Consult the table Classification data for storage and transport for some practical advice.

Paper questionnaires and data on paper

- The only data on a questionnaire which can be directly identified is the respondent number;
- For verification purposes, identifiers (like a name) may be present on the front page. The front page must not contain any research data. Immediately after verification, the front page must destroyed;
- Never store identifying data on images of the paper data!

Students and temporary co-workers without employment agreement
These research assistants or other project members are not allowed to have access to or process privacy sensitive data without a written and signed confidentiality agreement.

Finishing

- Check the data set(s) for (remaining) identifiers;
- Remover identifiers still present or de-identify these data;
- Destroy key files and administrative databases. The only exception for not destroying is a written consent of the participant or a legal obligation like Good Clinical Practice;
- Unsubscribe your project with the Centraal Meldpunt Gegevensverwerking, by sending an e-mail to privacy@vumc.nl

Privacy Definitions

- Anonymous data: data which can only lead to identification of the natural person after application of unreasonable means or disproportionate time and effort.
- Personal data: every fact about an identified or identifiable natural person;
- Personal data which can be directly identified: data that the researcher can use to directly identify, or in combination with more information can use to identity of the individual person.
- Personal data which can be indirectly identified: data which cannot be used to directly identity the individual person, but does make it possible for the researcher to identify the individual person without spending a disproportionate amount of time and effort;
- Data used for communications: data, such as last name, first name, initials, title, sex, date of birth, address, postal code, city, telephone number, email address, social media identifiers and other data needed for communication;
- Coded data: data which does not directly include identifying personal data and which have been encoded such that the identity of the individual person can only be determined by the intervention of the supplier or an independent third party and after application of the key to the code. Coded data are still personal data.

Amsterdam Public Health

Amsterdam UMC University Medical Centers | VU Vrije Universiteit Amsterdam | University of Amsterdam

Classification data for storage and transport

Storage and transport	Cabinet	Internal network	Sending external email	Encrypted** transport on mobile device (USB stick, laptop, tablet, etc.)	Cloud computing only allowed on Amsterdam UMC approved clouds***
Classification of data					
External public Published research, conducted lectures and presentations	No restrictions	No restrictions	No restrictions	No restrictions	No restrictions
Confidential Unpublished research, identifiable datasets	In a locked storage cabinet	In a secured project directory, only accessible for the project team	Allowed when encrypted documents	Allowed	Allowed with encrypted documents
Highly confidential Personal medical data, personal data of co-workers Video and sound recordings Key records, address records, respondent databases	In a locked storage cabinet and locked room	In a secured project directory, only accessible for the project team	Not allowed. Except when there is a written agreement approved by the head of the department and the file is encrypted	Only allowed when strictly necessary and the file is encrypted	Allowed with end to end encryption

Encryption tools
7 zip can be used to encrypt sensitive data. Use 265-aes as an encryption method and a long (at least 12 characters) password. Do not send the encrypted file and password both by email. Send the password through a different channel.
See here for instructions how to encrypt with 7 zip

SurfFile sender
SurfFile sender is available for encrypting and sending files to anybody.

Secure USB stick
Secure, encrypted,USB sticks, working under view can be ordered.

Data sharing tool
Surfdrive: Surfdrive is an approved cloud storage for public and medium sensitive data.

Audit questions

1. Are confidential details being collected in the project?
2. Which members of staff have access to confidential research data?
3. Has a confidentiality agreement been signed by all staff who have access to confidential research data?
4. Has the researcher taken the necessary measures regarding the safeguarding of files with confidential information?
5. Will separate, anonymized data be made available to individuals outside your organisation? If so, has a data transfer agreement been signed for this?
6. Are the input databases and other files with confidential information in a directory on the network?
7. Has the project been registered with the Privacy Officer? (Centraal Meldpunt Gegevensverwerking)

LINKS

	Link
Federa Goed Gedrag	https://www.federa.org/code-goed-gedrag
AMC Privacy en Informatiebeveiliging	http://intranet.amc.nl/web/organisatie/themas/overzicht-themas/privacywetgeving-en-gegevensbescherming.htm

IXA Contact	https://www.ixa.nl/about/contact-us/
Legal Research Support (AMC)	https://intranet.amc.nl/web/organisatie/domeinen/research/legal-research-support.htm
7-Zip to Encrypt Files and Folders	https://www.northeastern.edu/securenu/sensitive-information-2/how-to-use-7-zip-to-encrypt-files-and-folders/
VUmc CMG registration	https://intranet.vumc.nl/afdelingen-themas-1/clinical-monitoring-center/stappenplan-klinisch-onderzoek/goedkeuring/1.-centraal-meldpunt-gegevens-verwerking-cmg.htm

DOCUMENT HISTORY

Version	Status	Date	Name
1.1	Addition of trial registration and Population Screening Act (WBO)	SEPT2006	Dr. Michel Paardekooper
1.2	TIP non WMO project	22JAN2009	Dr. Michel Paardekooper
1.3	Translation into English and update	01JAN2009	Dr. Michel Paardekooper
1.4	Name change from Ready to Go to Law and Regulations and update	28JAN2013	Dr. Michel Paardekooper
2.0	Revision format and updated, addtion of data breach	12JUN2015	Dr. Michel Paardekooper
2.1	Minor textual corrections	20MAY2016	Dr. Michel Paardekooper

2.2	Addition of links to registration form for admission to sensitive data	16SEP2016	Dr. Michel Paardekooper
2.3	Updated, addition of serveral tools	22MAR2017	Dr. Michel Paardekooper
2.4	Updated into APH and added GDPR/AVG	13JUL2018	Dr. Michel Paardekooper
3.0	Revision	23FEB2021	Dr. Michel Paardekooper

DOCUMENT APPROVAL

Role	Name	Date
Project Leader	Dr. Seta Jahfari	29APRIL2021