Guidance on data collection for patient journeys

August 2021

This publication is intended as non-exhaustive, non-binding guidance on the processing of patient data by patient organisations. It is not intended to be, and should not be used as, a substitute for taking legal advice in any specific situation. EURORDIS will accept no responsibility for any actions taken or not taken on the basis of this publication. Each patient organisation is responsible for ensuring compliance with applicable laws, including the GDPR[1] and local data protection laws in respect of its own activities.

I. General principles on collection of personal data

The GDPR is applicable since 25 May 2018. Since then, companies and organizations should abide by the different rules and responsibilities imposed on them by the GDPR when processing personal data.

Please note that the concepts of 'personal data' and 'processing' are defined by the GDPR in a broad manner.

- *Personal data* means any information relating to an identified or identifiable natural person.[2]
- *Processing* means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means.[3]

Personal data goes further than just names and addresses. All data elements or data sets which allow to identify a natural person qualify as personal data. Only when the data do not allow to identify a person by any reasonable means, data are considered anonymous and consequently out of scope of the GDPR.

For example, if surveys are being carried out, the fact that no names or addresses are registered, does not mean that the survey does not contain personal data. The survey may be considered to contain personal data if you are able to identify the person to whom the data relate. In the context of rare diseases, we assume that in most cases you will be able to identify the natural person to whom the data relate even without having the name.

Personal data related to the health of a person is considered a special category of personal data and is subject to more stringent rules than 'normal' personal data.

When collecting data in the context of surveys or interviews, it is therefore of utmost importance to verify whether you are collecting personal data and/or health data. In case of doubt, we recommend – as a matter of precaution – to treat the data as personal data.

Non-compliance with the GDPR may result in administrative fines or other sanctions.

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
[2] Article 4.1 GDPR.
[3] Article 4.2 GDPR.

II. Recommendations on collection of personal data through individual interviews or through the EU Survey Platform for patient journeys

1. Process

1. Use a GDPR compliant consent form for interviews AND for surveys

If you wish to collect the data **through individual interviews or through the EU Survey Platform** and you collect personal data such as name, surname, email, age, date of birth, nationality and gender, and/or data concerning health such as diagnosis, symptoms disease, symptoms, diagnosis, physical condition, treatments and disease history, **you will need to collect GDPR compliant consent forms signed by all the respondents prior to the start of any data collection**.

A scanned version of the signed consent form will be sufficient to prove consent. However, if one of the respondents would want to dispute that they have provided consent, a scanned copy of their signed consent form will not be regarded as an indisputable proof. If you want to avoid any risk that the authenticity of the document can be disputed afterwards, you will need to keep either hard copies, or electronic copies which are signed by means of a qualified electronic signature (see the definition of a qualified electronic signature on page 13 here).

Examples

Should you wish to **interview people over the phone or to organise face to face or online meetings,** you will need to obtain signed consent forms prior to the interviews/meetings. It is recommended NOT recording the online meetings. If you do record these meetings, you would need to look at the telecoms laws of those countries and assess what is applying in this context.

Should you plan to send **online surveys (see section 2 below),** you can copy/paste the entire content of the consent form text at the beginning of the questionnaire and include a check box below which the participants need to check to confirm that they have read and understood the information and that they provide their consent for the processing of their personal data. This could read as follows:

> *"I have read and understood the [name of the document, e.g. Privacy Statement] and consent to the processing of my personal data as described therein".*

It is important that you obtain a copy of the consent which you can store. The EUSurvey tool is able to obtain a copy of the online signed consent forms.

2. Use the EU Survey Platform

If you want to use the EU Survey Platform to collect the data, first, create an EU login/ECAS account here and then connect to the EUSurvey tool. You will have to use your registered mobile phone for the two-factor authentication. Please contact Anne-Laure Aslanian anne-laure.aslanian@eurordis.org if you have any questions on how to create an EU login/ECAS account.

3. Delete all the data

Delete completely and safely all the data collected (e.g. paper copies should be destroyed, electronic back-ups should be wiped), either through individual interviews or through the EU Survey Platform, once you have developed the patient journey and do not keep records of the data.

2. Security measures

1. Basic approach

- Use protected internet connections secured by a password.
- Store interview responses in a password-protected database, at a minimum a password protected spreadsheet, which is only accessible by the persons who are collecting the information on a strict need-to-know basis. If personal data is stored in paper form, ensure it is kept in a secure location which is not accessible for non-authorised persons.
- Process the results in a computer protected with a strong password and antivirus software.
- Do not use or share the individual survey responses via email or any other means.

2. Additional recommendations

Where possible, it is recommended to take additional measures, such as for example measures to ensure that back-ups are available. **Please refer to the Annex I below that gives an overview of high-level security measures (this reference document was kindly provided by DLA Piper).** It is understandable that it may not be feasible for all patient organizations to implement all these measures, but it serves as a basis to consider what additional measures could be taken by each patient organization in order to increase its security level.

ANNEX I

Overview of high-level technical and organisational measures

by DLA Piper

Overview of high-level technical and organisational measures

Domain	Practices
Information Security Management and Governance	**Ownership for Security and Data Protection**. The patient organization has appointed a Risk & Security Officer responsible for coordinating and monitoring the security rules and procedures as well as data protection compliance. **Security Roles and Responsibilities**. Security responsibilities of personnel are formally documented and published in information security policies. **Risk Management Program**. The patient organization executes periodical risk assessments based on a formal risk management methodology.
Human Resources Security	**Confidentiality obligations.** The patient organization personnel with access to personal data are subject to confidentiality obligations, and these are formally integrated into employment contracts. **Termination.** The patient organization ensures according to formal security administration procedures that access rights are timely revoked upon termination.
Asset Management	**Asset Inventory**. The patient organization maintains an inventory of all computing equipment and media used. Access to the inventories is restricted to authorized patient organization personnel. **Asset Handling** - Personal data on portable devices are encrypted. - The patient organization has procedures for securely disposing of media and printed materials that contain personal data.
Information Access Control	**Access Policy**. The patient organization enforces an access control policy based on need-to-know and least privileges principles. **Access Authorization** -The patient organization has implemented and maintains an authorization management system that controls access to systems containing personal data.

	- Every individual accessing systems containing personal data has a separate, unique identifier/username. - The patient organization restricts access to personal data to only those individuals who require such access to perform their job function. - Technical support personnel are only permitted to have access to personal data when needed. **Authentication** - The patient organization uses industry standard practices to identify and authenticate users who attempt to access the patient organization network or information systems, including strong authentication. - Where authentication mechanisms are based on passwords, the patient organization requires that the passwords are renewed periodically and that they are at least eight characters long and sufficiently complex. - De-activated or expired identifiers/usernames are not granted to other individuals. - Accounts will be locked out in case of repeated attempts to gain access to the information system using an invalid password. - The patient organization maintains practices designed to ensure the confidentiality and integrity of passwords when they are assigned and distributed, and during storage.
Physical and Environmental Security	**Physical Access to Facilities**. - The patient organization limits access to facilities where information systems that process personal data are located to identified authorized individuals. - Physical access to data centers is only granted following a formal authorization procedure, and access rights are reviewed periodically. **Protection from Disruptions**. The patient organization uses a variety of industry standard systems to protect its data centers against loss of data due to power supply failure and fire.
Operations Security	**Data Recovery Procedures**

	- On an ongoing basis, but in no case less frequently than once a week (unless no data has been updated during that period), the patient organization maintains backup copies of personal data for recovery purposes. - The patient organization stores copies of personal data and data recovery procedures in a different place from where the primary computer equipment processing the personal data is located. **Malicious Software**. The patient organization maintains anti-malware controls to help avoid malicious software gaining unauthorized access to personal data. **Data Beyond Boundaries**. The patient organization standardly encrypts, or provides the mechanisms to encrypt, personal data that is transmitted over public networks. **Event Logging**. The patient organization logs access and use of its information systems containing personal data, registering the access ID, time and relevant activity.
Communications Security	**Network Segregation**. The patient organization has implemented a network segmentation policy and controls to avoid individuals gaining access to systems for which they have not been authorized. **Information Transfer**. Any transfer of personal data to third parties is only performed following the execution of a formal written non-disclosure agreement.
System Acquisition, Development & Maintenance	**Security Requirements**. Requirements for protecting data and systems are analyzed and specified. **Change Control**. The patient organization has implemented a formal change management process to ensure changes to operational systems and applications are performed in a controlled way.
The patient organization Relationships	**The Vendor Selection**. The patient organization maintains a selection process by which it evaluates the security, privacy and confidentiality practices of a sub-processor in regard to data handling.

	Contractual Obligations. The third party vendors with access to personal data are subject to data protection and information security obligations, and these are formally integrated into their contracts.
Information Security Incident Management	The patient organization maintains a record of security breaches with a description of the breach, the time, the consequences of the breach, the name of the reporter and to whom the breach was reported.
Business Continuity Management	**Disaster Recovery**. The patient organization maintains a disaster recovery plan for the facilities in which the patient organization information systems that process personal data are located. **Redundancy**. The patient organization's redundant storage and its procedures for recovering data are designed to attempt to reconstruct personal data in its original or last-replicated state from before the time it was lost or destroyed.
Compliance	**Security Reviews**. Information security controls are independently audited and reported to management on a periodical basis.