Good Practices in Informed Consent and Data Management in European Reference Networks for Rare Diseases

An overview of good practices for health data collection and processing in the context of European Reference Networks for Rare Diseases

December 2017

This document has been prepared by FTI Consulting (Petra Wilson & Isabelle Andoulsi) as a deliverable of contract SANTE/2016/B3/061.

The information and views set out in this publication are those of the author(s) and do not necessarily reflect the official opinion of the Commission. Neither the Commission nor any person acting on the Commission's behalf may be held responsible for the use which may be made of the information contained therein.

Table of Contents

INTRODUCTION **4**

MEETING THE LEGAL REQUIREMENTS FOR PROCESSING HEALTH DATA IN THE ERN CONTEXT **6**

Introduction *6*
Providing information on the data to be collected and its intended use *7*
Recording Consent *7*
Valid basis for processing data *8*
Data processing in accordance with adequate security and administrative processes *8*
Duties of the data controller *8*
Duties pertaining to de-identified data *8*
Providing Patient Access and Portability *9*
Duties of notification of breach *10*

THE RELATIONSHIP BETWEEN THE CLINICAL PATIENT MANAGEMENT SYSTEM AND THE ERN MEMBER WITH RESPECT TO DATA SHARING **11**

Introduction *11*
The age of capacity to consent *11*
The data of deceased persons *11*
Data use for research *12*

GLOSSARY OF KEY DATA PROTECTION TERMS **14**

ANNEX 1 ..... **16**

A REVIEW **16**

OF **16**

DATA SHARING CONSENT FORMS **16**

TO IDENTIFY **16**

GOOD PRACTICES **16**

INTRODUCTION **17**

Consent to share data for research and treatment of specific named diseases and conditions *17*
Regional Cancer Network ONCO Nord Pas-de-Calais *18*
Consent form used in the speech therapy research *19*
Consent for the sharing of data for the evaluation of medical products, care or patient safety *20*
Consent to share medical data with a legal advisor *21*
Consent to access electronic health records or medical records *21*
Consent to support social care assistance *22*
Multiple choice consent forms *23*
Consent in the context of medical fees reimbursement *23*

Introduction

The European Reference Networks for Rare Diseases (ERNs) were created as a result of Article 12 of the Directive on the application of patient's rights in cross-border healthcare[1], as a way of addressing the needs of patients with rare diseases in Europe, and more particularly to facilitate sharing and pooling of expertise in rare diseases across the EU. The ERNs are therefore envisaged as virtual networks of healthcare providers and professionals supported by a shared platform through which data may be shared safely.

The concept of the ERNs is firmly rooted in eHealth, and, as such, is focussed primarily on electronic sharing of expertise, rather than the physical movement of patients. However, the ultimate movement of a patient with a rare disease to be treated by an ERN member located in another Member State is not excluded. If care is provided by an ERN Member who is not located in the Member State where the patient is resident, reimbursement will be regulated under the rules of Directive 2011/24 EU on patients' right to cross-border care or Regulation 883/2004[2] on the coordination of social security systems. In terms of legal liability for the quality care, under both the Directive and the Regulation this remains the responsibility of the legal entity providing the care. The advice provided within an ERN between healthcare professionals does not attract either a legal or financial responsibility outside the one already existing between the treating physician and the patient.

Building on the provision in the Directive on the application of patient's rights in cross-border healthcare, ERNs were further defined by the Commission Delegated Decision of 10 March 2014[3]. This delegated legislation sets out the criteria and conditions that must be fulfilled by ERNs. In this delegated decision, one can see that ERNs and the concepts of data protection are closely linked. Recitals 9 and 12 of the delegated decision state that:

> *(9) The ability to have an efficient and secure exchange of health data and other patient information as well as personal data of the healthcare professionals in charge of the patient is a crucial aspect for the successful functioning of the Networks. The exchange of data should in particular take place in accordance with the specified purposes, necessity and legal grounds for the processing of data and be accompanied by appropriate safeguards and rights of the data subject. Personal data should be processed in compliance with Directive 95/46/EC of the European Parliament and of the Council.*
>
> *[….]*
>
> *(12) In order to ensure the exchange of personal data in the context of the Networks, procedures concerning informed consent for processing this data could be simplified by using one single common consent model that needs to be subject to the requirements set out in Directive 95/46/EC with regard to the consent of the data subject.*

---

[1] Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross-border healthcare (OJ L 88, 4.4.2011, p. 45)

[2] Regulation (EC) No 883/2004 of the European Parliament and of the Council of 29 April 2004 on the coordination of social security systems (OJ L 166, 30.4.2004, p. 1)

[3] Commission Delegated Decision 2014/286/EU of 10 March 2014 setting out criteria and conditions that European Reference Networks and healthcare providers wishing to join a European Reference Network must fulfil (OJ L 147, 17.5.2014, p. 71)

Annex II article 1 (a) (v) of the Delegated Decision specifies that the common consent model should ensure that:

> *(v) […] informed consent given freely, unambiguously and explicitly by the subject or his/her legal representative after being informed of the purpose, nature, significance and implications of the use of his/her personal and health data, if personal health data is exchanged under this Delegated Decision, and being informed of his/her rights under the applicable data protection rules. The given consent should be duly documented.*

The purpose of this paper is to provide further background information on the concepts integrated into the Standardised Consent Form, which have not been described within the Guideline and Toolkit. While the Guideline and Toolkit were designed to be used by healthcare professionals tasked with requesting patient consent to sharing data in an ERN, this Review of Good Practices is targeted not only at those healthcare professionals, but also the governing bodies of ERNs and the healthcare institutions which are members of ERNs.

Annex 1 of this deliverable provides a review of a number of consent forms which were consulted in the process of drafting the ERN Standardised Consent Form, highlighting particular elements of good practice they display. The review provides links to a range of different consent forms from which lessons of good and less good practices were drawn.

The review considers nineteen different consent forms, and outlines the key learnings drawn from each one. The layout and wording of these forms can inspire best practices in order to obtain a freely given informed consent from the patient, and may be of use where an ERN Member is considering adapting the Standardised Consent Form to its Member State's legislation requirement or adopting / updating its own informed consent procedures for any other purpose.

Meeting the Legal Requirements for Processing Health Data in the ERN Context

Introduction

The Commission Delegated Decision of 10 March 2014, which established the rules of operation of the ERNs references compliance with the 1995 Data Protection Directive[4]. However, given that this legislation will be replaced the General Data Protection Regulation (GDPR)[5] in May 2018, the present document focuses primarily on the GDPR although reference is made to the Directive where relevant.

The Data Protection Directive, *prima facie,* prohibits the processing of sensitive data and more particularly data concerning health (Article 8, paragraph 1). However, paragraph 2 of Article 8 provides for derogations to this prohibition including the derogation that the processing of health data shall be possible when "*the data subject has given his explicit consent to the processing of those data (…)"*.

In the GDPR, the same principle applies. Article 9, paragraph 1 of the GDPR states that "(…) *the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health (…) shall be prohibited*". However, in application of paragraph 2 (a) of Article 9, the collection and processing of such data shall be possible where the data subject has given his/her explicit consent to the processing of those personal data for one or more specified purposes.

In addition to the explicit consent, other derogations exist to allow the processing of health information. Accordingly, health data may also be collected and processed, if to do so is:

- necessary to protect the vital interests of a data subject who is physically or legally incapable of giving consent (Article 9(2)(c));
- necessary for the purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services on the basis of Union or Member State law or a contract with a health professional (Article 9(2)(h)); and
- necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of healthcare and of medicinal products or medical devices (Article 9(2)(i)).

These provisions expand the equivalent provision in the Data Protection Directive and address acknowledged gaps in that Directive, by providing a formal legal justification for regulatory uses of healthcare data in the health and pharmaceutical sectors, and by providing for the sharing of health data with providers of social care. Note however that the latter two conditions require obligations of professional confidentiality to be in place by way of additional safeguard.

[4] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ L 281, 23.11.1995, p. 31)

[5] 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) (OJ L 119, 4.5.2016, p. 1)

Therefore, while processing of health data is *prima facie* prohibited, both the Directive and the Regulation provide that they may be processed in the circumstances listed above. For ERNs, the derogation to be applied will be the one of explicit consent. It is unlikely that an ERN will process data using the emergency derogation as such emergencies will usually be treated at national level. However, it is of course possible that a patient might lack the physical or intellectual capacity to give consent, while the expertise of a clinician in the ERN is needed to treat that patient. In such cases, the ERNs might indeed make use of the emergency processing derogation.

Providing information on the data to be collected and its intended use

Consent must always be requested. Where possible this request should be made directly to the patient, but in some cases a legal representative or guardian may also be consulted (this is described in more detail below).

Because consent must be informed, it is important that the patient has some background information and also that he or she should be able to ask questions to the healthcare professional requesting consent about:

- the nature of the data to be collected;
- its intended use;
- details of who will have access to the data;
- details about how the data will be stored; and
- the contact details of the data controller.

The legislation does not require that patients are provided with written information, but good practice indicated that some form of written information is advisable.

However, such information must be understandable to the patient. It should be easy to read and written in simple language.

The ERN Standardised Consent Form has been drafted to conform to such standards. However, it may be necessary to make large print available for patients with visual impairment.

In addition, the patient must be given adequate time to read the form and should not be pressured. The healthcare provider charged with presenting the form must choose the right moment to do so, and also, assist the patient in reading the form if necessary.

Recording Consent

Organisations must be able to prove that consent has been given. Annex II article 1 (a) (v) of the Delegated Decision specifies that *"the given consent should be duly documented."* For this reason, the ERN Standardised Consent Form provides for a written signature. Although a written signature is not legally required, it is the simplest method by which to show that consent was duly requested and given.

While it is not a legal requirement that a patient should receive a copy of the consent form they have signed, it is good practice to be able to provide patients with such a copy, either in paper or via an electronic link in an on-line information portal.

Valid basis for processing data

In order to comply with the rules of data protection, every organisation must be able to prove that they have the right to process data; consent for illegal processing does not make it legal. In the ERN context, this should not present any issue, since processing data for the purposes of providing medical care or undertaking *bona fide* research are adequate legal grounds for data processing.

Data processing in accordance with adequate security and administrative processes

Organisations must be able to show that they are processing data in accordance with good security and administrative practice. This requirement means that adequate state-of-the-art data storage and security systems are in place. This includes being able to identify the patient who has consented to data processing, which kind of data processing activities have been consented to, when the consent was given, and the way the consent has been granted. The Standardised Consent Form has been drafted to allow a care provider to demonstrate all these factors.

Duties of the data controller

It is the responsibility of the data controller for any given data processing activity to ensure that the standards described above are met. In the context of ERNs, there are several data controllers.

The data collected and stored by an ERN member, who is physically providing care to the patient, will be held according to the rules and processes for collecting and storing patient data in the ERN member's institution. This storage falls outside the legal ambit of the ERN and is covered by the internal rules of the organisation and the national legislation of the country in which it is established.

When data is made available for sharing in an ERN consultation between ERN members, it is shared through the ERN Clinical Patient Management System (CPMS).

The European Commission has contracted with an external provider for this system, and accordingly has accepted the role of data co-controller for the de-identified data held on that system. The responsibility is shared with the provider of the CPMS who is also a data co-controller for the CPMS. This means that they share the responsibility for ensuring that data sharing facilitated by the CPMS is covered by adequate standards of security.

Duties pertaining to de-identified data

Any *"personal data",* which is defined as *"information relating to an identified or identifiable natural person 'data subject'",* falls within the scope of the Regulation. The Regulation does not

apply to data that "*does not relate to an identified or identifiable natural person or to data rendered anonymous in such a way that the data subject is no longer identifiable.*"

The data shared in the ERNs will be de-identified. The term de-identification as used in the Standardised Consent Form is similar to the concept of pseudonymisation as used in the GDPR. The GDPR defines pseudonymisation as *"the processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information, as long as such additional information is kept separately and subject to technical and organizational measures to ensure non-attribution to an identified or identifiable individual"* (Article 4(3)(b) GDPR).

It is important to note that de-identification (or pseudonymisation) is not the same as making data anonymous. If data are truly anonymous, as defined by the GDPR, they fall outside the ambit of the GDPR and accordingly no consent is needed to sharing such data. However, the GDPR considers data to be anonymous only when it cannot be identified by any means *"reasonably likely to be used* (...) *either by the controller or by any other person"* (Recital 23 GDPR). Thus, even if a given healthcare professional or researcher does not have access to the tools to re-identify data, such data may still be regulated under the GDPR, if it could be re-identified with reasonable effort.

Furthermore, even if it could be argued that the data shared in the ERN are sufficiently well de-identified to be legally classified as anonymous, it is important to note that the Commission Delegated Decision on the operation of ERNs states that informed consent is provided for the sharing of data in ERNs.

Providing Patient Access and Portability

According to the GDPR, as well as the previous Directive, patients have a right to access data held about them and to request correction to any errors they might find. The organisation holding patient data must therefore be able to provide access to the patient records and also to respond to requests for correction.

In the context of ERNs this means that the ERN Member treating the patient must be able to explain which data held by that Member have been shared, noting of course that at the time of sharing the data was de-identified.

The ERN Member must be able to provide access to the nominative data held by the Member and in collaboration with the CPMS provide access to an extract of the ERNs data as shared between ERN Members for the purposes of discussing the given patient's care.

The right to data portability is a new patient right introduced in Article 20 of the GDPR. It is a right which is closely related to, but differs from, the right of access. It allows patients to receive the data which they have provided to a healthcare professional, in a structured, commonly used and machine-readable format, and to transmit them to another healthcare professional if they choose to do so. The purpose of this new right is to empower the patient and give him/her more control over the personal and medical data concerning him or her.

ERN members should therefore be able to provide, free of charge, to each patient (or directly to another organisation treating the patient, if requested to so by the patient), his/her personal and medical data in a structured, commonly used and machine readable form (which means that the information is structured so that another organisation can use the data). Organisations must be ready to respond to patients' requests without undue delay. The GDPR does not define undue delay, but guidance from some Member States indicates that the organization must provide the patient with a timeframe within which an answer shall be provided and if this period is lengthy, to explain the reasons for the time taken.

Duties of notification of breach

Unlike Directive 45/96, which was silent on the issue of data breach, the GDPR introduces a duty on all organisations to report certain types of data breach to the relevant supervisory authority, and in some cases to the individuals affected.

In the event that an organisation incurs a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed (thus not just personal data loss), the supervisory authority of the Member State must be informed of such a breach. Organisations should inform the relevant supervisory authority of a breach only in cases where such a breach is likely to result in a risk to the rights and freedoms of individuals, which means that when left unaddressed, such a breach is likely to have a significant detrimental effect on individuals – for example, result in discrimination or loss of confidentiality.

Organisations should inform the supervisory authority without undue delay and, where feasible, not later than 72 hours after having become aware of the data breach. Organisations should include, at least, the following information to their notification:

- a description of the nature of the personal data breach, including the number and categories of data subjects and personal data records affected;
- the data protection officer's contact information;
- a description of the likely consequences of the breach; and
- a description of how the organisation plans to address the breach, including any mitigation efforts.

In the context of ERNs the duty to report such a breach will fall on the data controllers of the CPMS. However, it is important to remember that each ERN member holds the same responsibility towards the patients whose records they hold, and must assume the required steps of notification if they have suffered a data breach.

The Relationship between the Clinical Patient Management System and the ERN Member with respect to data sharing

Introduction

A core objective of the GDPR is to create the legal framework for the seamless cross-border delivery of all kinds of data services essential to a digital single market. The coordination and harmonisation of national regulatory regimes are indispensable in achieving this goal. However, for as long as there is not full harmonisation across different regimes, there remains a risk that service providers have to comply with different national regulation in different EU countries.

However, because the organisation of health systems is a matter of Member State (rather than EU) competence, the GDPR provides for several derogations that may mean that there are still variations across EU. On the basis of Article 23 of the GDPR such derogations may be adopted in cases of national interests in public health or processing for archiving purposes and for scientific or historical research and statistical purposes.

Since ERNs are designed to be an information forum for healthcare providers, rather than a care provision mechanism, many of the issues related to variations between Member State interpretations of the GDPR will not present any problem for ERN Members. However, ERN Members should have a good understanding of three issues related to:

- the age at which consent may be given;
- the treatment of data concerning a deceased patient; and
- the data use for research purposes.

The age of capacity to consent

The GDPR leaves some latitude to the EU Member States on the issue of providing for the conditions applicable to a child's consent in relation to information society services. Paragraph 1 of Article 8 states that where the lawfulness of a processing should be established *"in relation to the offer of information society services directly to a child, the processing of the personal data of a child shall be lawful where the child is at least 16 years old. Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child. Member States may provide by law for a lower age for those purposes provided that such lower age is not below 13".*

The data of deceased persons

Data Protection Directive does not mention data of the deceased in any context, and Recital 27 of the GDPR states that the Regulation does not apply to the personal data of deceased persons. However, it does provide that Member States may provide for rules regarding the processing of personal data of deceased persons. Generally, the Member States have historically provided for only very limited data protection rights to the data of a deceased person.

In the English common law system, there is a long recognised principle of *actio personalis moritur cum persona* (personal causes of actions die with the person) and in France the Appeal Court held that *"the right to act in respect of privacy disappears when the person in question, the sole holder of that right, dies"* (SA Editions Plon v Mitterand). Furthermore, according to the European Court of Human Rights case law, Article 8 of the European Convention on Human Rights grants protection only to the living.

It is however noteworthy that rare diseases research will often need to use the data of deceased patients, and that these data will often include genetic information that may in turn reveal information about living descendants. The question arises therefore if in the case of rare diseases special attention should be paid to the data of deceased patients.

Data use for research

Achieving the right balance between the interests of the medical and scientific research community and the patient is an important aim of the GDPR and its preceding legislation. This is of course of great importance to ERNs, because a core objective of ERNs is to reinforce research and epidemiological surveillance by means of the development of registries and by providing training of health professional in the diagnosis and treatment of patient with rare diseases (Article 12, paragraph 2, (e) Cross Border Care Directive).

Article 89 of the GDPR directly addresses the issue of data processing for research in the following terms:

> *"(1) Processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, shall be subject to appropriate safeguards, in accordance with this Regulation, for the rights and freedoms of the data subject. Those safeguards shall ensure that technical and organisational measures are in place in particular in order to ensure respect for the principle of data minimisation. Those measures may include pseudonymisation provided that those purposes can be fulfilled in that manner. Where those purposes can be fulfilled by further processing which does not permit or no longer permits the identification of data subjects, those purposes shall be fulfilled in that manner.*
>
> *(2) Where personal data are processed for scientific or historical research purposes or statistical purposes, Union or Member State law may provide for derogations from the rights referred to in Articles 15, 16, 18 and 21 subject to the conditions and safeguards referred to in paragraph 1 of this Article in so far as such rights are likely to render impossible or seriously impair the achievement of the specific purposes, and such derogations are necessary for the fulfilment of those purposes".*

Accordingly, provided Member States achieve an appropriate balance between the right of each data subject and the specific interest of research for rare diseases, and provided they adopt the needed safeguards, they will able to adopt derogations from the data subjects' rights (right of access, right to be forgotten, right to restrict processing and right to object processing), for research purposes in ERNs.

However, at the time of writing in early 2017, no notification of such special derogation has been received by the European Union, and therefore ERN Coordinators will need to remain vigilant and ensure that ERNs members inform the Coordinators of any national variations that are adopted. It will also be important for ERN Coordinators and the ERN Boards to consider if special rules are needed for ERNs and to work with national regulators accordingly.

This is in fact specifically provided for in Annex I to the Commission Delegated Decision, dedicated to the criteria and conditions to be fulfilled by the ERNs, in order to make a contribution to research (to fulfil the requirement set out in point (iv) of Article 12, paragraph 4 (a) on the application of patients' rights in cross-border healthcare), which states that each ERN must:

(a) identify and fill research gaps;
(b) promote collaborative research within the Network;
(c) reinforce research and epidemiological surveillance through setting up of shared registries.

Moreover, in Annexe II to the same Delegated Decision, applicant ERN partners are required to:

(i) have the capacity to provide academic university or specialised level training;
(ii) have human, technical and structural capacity, skill mix and resources;
(iii) have research capacity, and demonstrate research experience or production in the area of expertise of the Network, at national and international level; (and)
(iv) carry out teaching and education activities related to the area of expertise aimed at improving the knowledge and technical capacity of the healthcare providers involved in the same chain of care within and outside the provider facility, such as continuing medical education and distance learning.

It is clear therefore that ERNs have a strong research element and that clinical research facilities have a clear role in ERNs. They will provide the clinical, laboratory, regulatory and operational support for clinical research studies and will also often play a key role in supporting patients and healthcare professional throughout their involvement in clinical research. It is key therefore the clinical research facilities play their part in ensuring that data protection in ERN research is assured and that patients are fully and properly informed about the research which will , or may, be undertaken using the data collected specifically for research purposes,[6] as well as data collected in the process of care.

[6] Under Article 89 when data are processed for research purposes, if consent has been obtained for collecting the data such data may be reuse for further research if such research falls broadly in the same category as the research purpose for which the data was originally collected. Therefore consent given for the collection of data within an ERN will usually be sufficient for any further research conducted within that ERN.

Glossary of key data protection terms

Anonymisation: The technique of processing personal data so that it can no longer be attributed to a specific individual. The technique is almost irreversible as efforts to reattribute personal data to a specific data subject are numerous and costly in times and effort.

Clinical Research Facility (CRF): The term refers to any designated medical facility used to conduct clinical research, such as hospital or medical clinic. These facilities have been used to perform clinical trials of various medical procedures.

Data controller: A person or body, alone or jointly, which determines the purposes and means of processing personal data.

Data processor: An entity which processes the data on behalf of the data controller. The European Directive 95/46/EC previously governed the processing of personal data in the EU and will now be replaced by the GDPR. DPO A Data Protection Officer – whose appointment is obligatory under the GDPR where: (i) processing is carried out by a public authority; or (ii) the "core activities" of a data controller / data processor either: (a) require "the regular and systematic monitoring of data subjects on a large scale" or; (b) consist of processing of special categories of data or data about criminal convictions "on a large scale".

Epidemiological surveillance: epidemiological surveillance is according to the World Health Organization (WHO), "the continuous, systematic collection, analysis and interpretation of health-related data needed for the planning, implementation, and evaluation of public health practice." Public health surveillance may be used to "serve as an early warning system for impending public health emergencies; document the impact of an intervention, or track progress towards specified goals; and monitor and clarify the epidemiology of health problems, to allow priorities to be set and to inform public health policy and strategies.

Explicit consent: also known as express or direct consent — means that an individual is clearly presented with an option to agree or disagree with the collection, use, or disclosure of personal information.

Grandfathering clause: Is a clause exempting certain pre-existing classes of people or things from the requirements of a piece of legislation.

Hippocratic Oath: an oath stating the obligations and proper conduct of doctors, formerly taken by those beginning medical practice.

Personal data breach: This means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Personal data: This is any information relating to an identified/ identifiable, natural person, a 'data subject'. A data subject is a natural person, who can be identified, or is identifiable, directly or indirectly.

PIA - Data Protection Impact Assessment: The GDPR imposes a new obligation on data controllers and data processors to conduct a Data Protection Impact Assessment (otherwise known as a privacy impact assessment, or PIA) before undertaking any processing that presents a specific privacy risk by virtue of its nature, scope or purposes.

Process: This is defined widely to cover any operation or set of operations which is performed on personal data or sets of personal data, whether or not by automated means. Examples of processing include the collection, recording, organisation, storage, use and destruction of personal data.

Pseudonymisation: The technique of processing personal data so that it can no longer be attributed to a specific individual without the use of additional information, which must be kept separately and be subject to technical and organisational measures to ensure non-attribution.

Sensitive data: The GDPR has extended the definition to include both biometric and genetic data.

Supervisory authority/lead authority: Supervisory authorities are national data protection authorities, empowered to enforce the GDPR in their own Member State.

Annex 1

A Review

of

data sharing consent forms

to identify

Good Practices

Introduction

The objective of this review is to share the range of consent forms which were reviewed by the consultants and at the ERN workshops in the development of the Standardised ERN Consent Form. This review provides links to a range of different consent forms which were in use at the time the ERN Standardised Consent Form was developed, and from which lessons of good and less good practices were drawn.

The review considers nineteen different consent forms, and outlines the key learnings drawn from each one. The consent forms reviewed cover a range of issues for which consent was sought (1-6) as well as one multiple-choice form which sought to cover a wide range of potential data categories and uses.

1. Research on and treatment of specific diseases.
2. Consent forms drafted in the context of the evaluation and improvement of medical products, medical care or patient safety.
3. To share medical data with a solicitor.
4. To obtain access to electronic health records or medical records.
5. For the patient to benefit from care assistance.
6. A multiple choices consent form.
7. A form drafted in the context of medical fees reimbursement.

The nineteen forms have been selected from a range of Member States of the European Union (Belgium, France, Italia, Spain and the United Kingdom). However, such forms could not be found in all EU countries. Some forms are also drafted by organisations based outside of the territory of the European Union (Switzerland and the United States).

The layout and wording of these forms can inspire best practices in order to obtain a freely given informed consent from the patient. The layout and wording of these forms can inspire best practices in order to obtain a freely given informed consent from the patient, and may be of where an ERN member is considering adopting or updating its own informed consent procedures.

Consent to share data for research and treatment of specific named diseases and conditions

Regional Cancer Network OncoPaca-Corse

Website: www.oncopaca.org
URL:
https://www.oncopaca.org/sites/default/files/2016_formulaire_modele_regional_recueil_consentement_patient_dcc_rrc_tp.pdf

Description: The Regional Cancer Network OncoPaca-Corse seeks patients' consent in order to enable a study of each patient's medical file in multidisciplinary commissions to promote a better coordination of cancer medical care in general. It also seeks patients' consent in order to process patients' medical data for cancer research.

Good practices: The form contains precise explanations about the data controller, how to contact him and about the purposes of processing patient's medical data. It also contains a developed part

on data subjects' rights and separate part for obtaining patients' consents on the different proposed medical data processing.

Regional Cancer Network ONCO Nord Pas-de-Calais
Website: www.onco-npdc.fr
URL: https://media.onco-npdc.fr/consentement-new-v05-21783.pdf

Description: Similarly to the Regional Cancer Network OncoPaca-Corse, the Regional Cancer Network ONCO Nord Pas-de-Calais seeks patients' consents in order to enable a study of each patient medical file in multidisciplinary commissions towards a better coordination of cancer medical care in general. It also seeks patients' consents in order to process patients' medical data for research against cancer. The layout of the consent form differs slightly from the one mentioned above as more space is dedicated to the patient information and less to the consent itself. The content of the form is more or less the same as the one above.

Good Practices: It is states that if the patient is not willing to consent to the processing of his/her data, his/her treatment shall not be of lower quality, as consequence of his/her refusal to consent. This addition is a plus point in order to obtain a free patient consent for the processing of his/her medical data.

FAPA – Belgian Polyposis Project
Website: www.belgianfapa.be
URL:
https://www.belgianfapa.be/sites/default/files/consentement%20Lynch%20partie%201%20FR_0.pdf

Description: The Belgian Polyposis Project (and more specifically the Hereditary Colorectal Cancer Project) seeks to create a national registry in order to identify patients suffering from non-polyposis colorectal cancer and to collect and process their data for research and statistics. The consent form of this project contains, in a first part, a developed description of the purposes of collecting and processing patient's medical data. The second part of the form is dedicated to the patient freely given consent. An annex is then dedicated to patient's rights.

Good Practices: The unusual construction of this form, where the patient gets at first to consent to the processing of his/her data and is then informed about his/her rights. However, the consent form is a six pages document, which could be considered a bit too long.

Fresenius Medical Care Italia S.p.A.
Website: www.nephrocare.fr
URL:
https://www.nephrocare.fr/fileadmin/user_upload/assets/documents/fr/1_Holiday_Dialysis__Patient_Information_Consent_Form_ITA-FR.pdf

Description: Fresenius Medical Care Italia S.p.A. provides the Italian Kidney Cate Coordination Center and is responsible for collecting and processing personal data linked to the coordination of dialysis treatments on vacations spots for patients. Its consent form aims to collect patient personal data in order to coordinate and facilitate dialysis treatments when the patient is on holiday and thus far from his/her usual treating hospital.

Good Practices: The form has a very clear layout over three pages. The patient is given all the needed information, about the data controller, about his/her medical condition, the hypothesis of being sick when on holiday and all his/her personal data rights, before giving his/her consent.

The form also has a well-drafted and specific part dedicated to the transmission of personal data outside the Italian territory and even outside the European Union territory. The form layout thus ensures that the patient consent is informed, specific and freely given.

European Cystic Fibrosis Society
Website: www.ecfs.eu
URL: https://www.ecfs.eu/sites/default/files/general-content-files/working-groups/ecfs-patient-registry/SamplePatientConsentForm.pdf

Description: The consent form used by the European Cystic Fibrosis Society is a one-page document asking for the consent of patients with this specific disease to collect and use their medical data for research.

Good Practices: the form contains the inclusion of the parent/guardian for the consent of underage patients.

However, the form does not contain any details about the registry and its uses, or the purposes of collecting and processing patients' data, but a descriptive sheet is given to each patient with the form. Furthermore, the form does not contain any information about the patient rights, but the right to

Consent form used in the speech therapy research

University of Geneva, Faculty of Psychology and educational sciences
Website: www.unige.ch
URL: https://www.unige.ch/fapse/logopedie/files/7414/1285/1104/declaration-consentement.pdf

Description: This is a one page consent form used by the Faculty of psychology and educational sciences of the Geneva University in specific research projects.

Good Practices: The plus point of this consent form is the inclusion of the parent for the consent of underage patients.

However, it does not provide patients with information on the data controller or the purposes of collecting and processing their personal data. This information is included in another document given separately to each patient.

Switzerland is not bound by the GDPR, but it is worth noting that in order to conform to the GDPR more details of data use and the data controller would be required.

Consent for the sharing of data for the evaluation of medical products, care or patient safety

DePuy International Limited
Website: http://emea.depuysynthes.com/
URL: https://webcache.googleusercontent.com/search?q=cache:et-o3SQwEIEJ:https://www.depuysynthes.com/asrrecall/sites/default/files/fr/DPYOUS_12%2520ASR%2520Patient%2520Consent%2520Form_BEFR.docx+&cd=1&hl=fr&ct=clnk&gl=be

Description: The consent form, developed by DePuy International Limited, is used in order to collect and processed medical data from patients who have received a Depuy International Limited implanted medical product. The purpose of the data collection is mainly in order to evaluate patient satisfaction after the surgery.

Good Practices: The consent form contains wide information about the data controller, the specific purposes of the personal data collecting and processing and the transfers of personal data within the European Union and abroad.

Furthermore, the utilisation of the formulation "I understand that" or "I consent to" can be seen as positive and patient empowering. Moreover, the patient has the facility of barring one part of the document (see point 10) and to ask for an independent opinion where having questions about the form or doubts about signing it or not.

National Joint Registry
Website: www.njrcentre.org.uk
URL:
http://www.njrcentre.org.uk/njrcentre/Portals/0/Documents/England/Patient%20consent/NJR%20Patient%20Consent%20Form%20English%20FINAL%202014m.pdf?ver=2014-11-06-152401-640

Description: The role of the National Joint Registry (NJR) for England, Wales and Northern Ireland is to improve patient safety and monitor the results of joint replacement surgery. After a joint replacement surgery, each patient can be included in the registry in order to find out which are the best performing artificial joints and the most effective surgery.
Good Practices: The consent form drafted by the NJR (a two pages document) gives the patient all the information he/she needs to receive following the GDPR structure. The plus point of this consent form is that it is a very dynamic document. The vocabulary used makes it easy to read and understand for patients. All parts of the document contain proper and proportionate information. Finally, the consent part gives each patient the opportunity of consenting or not to the collecting of his/her personal data.

Alternative Care for Fragile Aged Persons Project (Inami)
Website: https://www.inami.fgov.be
URL: https://webcache.googleusercontent.com/search?q=cache:OQv-FUUO3VQJ:https://www.inami.fgov.be/SiteCollectionDocuments/convention-financement-soins-personnes-agees-annexe1.docx+&cd=3&hl=fr&ct=clnk&gl=be

Description: The National Institute for sickness/invalidity insurance (Inami) collects personal data from fragile aged persons in order to establish for each aged person a specific care plan. The consent form developed in the framework of this research project, presents in a first part an information

note for the patient to be aware amongst others of the finalities of the personal data processing, the data controller identity, etc.

Good Practices: Despite the fact that the form is pretty long (five pages), a clear layout renders it easy to read and to understand. A plus point of the form is the fact that it contains a specific part dedicated to the consent of aged persons that are not capable of giving their consent to the processing of their personal data. The second plus point of the form is that each patient can choose amongst a list of healthcare professionals which of them cannot have access to his/her personal data.

Consent to share medical data with a legal advisor

Law Society of Scotland and British Medical Association
Website: https://www.bma.org.uk
URL: https://www.bma.org.uk/-/media/files/pdfs/employment%20advice/ethics/bmalawsocietyconsentformmarch2017.pdf?la=en

Description: The consent form developed by the Law Society of Scotland and the British Medical Association asks for the client's consent to share his/her medical data with his/her lawyer as he/she may need health/employee personal data in order to pursue a case properly. This form seeks the consent of the client, the healthcare professional and the solicitor in order for medical information to fully flow from the healthcare professionals to the solicitors.

Good Practices: The form presents in a clear and concise way (1 page) the obligations of each actor in the medical data exchange system.

Consent to access electronic health records or medical records

HEALTHeLINK
Website: www.wnyhealthelink.com
URL: http://www.wnyhealthelink.com/files/consent/Patient_Consent_Form.pdf

Description: The consent form developed by the non-for-profit organization called HEALTHeLINK allows a patient to decide whether to allow Participating HEALTHeLINK Providers and Payers involved in his/her care to see and obtain access to his/her electronic health records for treatment and/or care management purposes.

Good Practices: This consent form allows each patient to choose to whom he/she gives access to his/her electronic health records and to introduce a difference in access to information between diverse healthcare professionals.

Danetre Medical Practice
Website: https://www.danetremedicalpractice.co.uk
URL: https://www.danetremedicalpractice.co.uk/wp-content/uploads/2013/09/patient-Access-Protocol.pdf
Description: The Danetre Medical Practice created a general information kit about access to medical records, an information leaflet about patient access to medical records and two separate forms in

order for the patient to access his/her medical records on the one hand, and for another person to access his/her medical records on the second hand.

Good Practices: Although this information package is very comprehensive, the form as a whole may be too complex for many patients.

It should also be noted that the form specifically mentions the fees patients should pay in order to obtain copies of their medical records. Caution should be exercised that such fees are reasonable and proportionate.

TTP
Website: www.tpp-uk.com
URL: https://www.tpp-uk.com/resources

Description: TTP is a UK based IT company dedicated to delivering healthcare software through innovative products. The consent form created by this IT company, for New Springwells Practice seeks patient consent to give access to his/her medical record to different care team members in the medical practice treating him/her and outside that medical practice.

Good Practices: The form is very short, visual and readable making uses of different fonts in order to give the patient the needed information. The adding of graphs is also very useful for the patient in order for him/her to understand what he/she is consenting to. This consent form is interesting as it provides for different consents for sharing medical records outside the medical practice treating the patient and for sharing medical records recorded at other care teams with the team of the medical practice treating the patient.

The British United Provident Association Limited (BUPA)
Website: www.bupaglobal.com
URL:
https://webcache.googleusercontent.com/search?q=cache:KwQKbLZfQqwJ:https://www.bupaglobal.com/-/media/files/pdfs/2015/buck-consultants-ppa/bin-generic-data-consent-form-jul14.pdf%3Fla%3Den+&cd=1&hl=fr&ct=clnk&gl=be

Description: The consent form developed by BUPA aims at obtaining the data subject informed consent to share his/her medical information with a listed intermediary in order to manage his/her policy insurance.

Good Practices: The form is simple and a glossary included on page 2 provides the data subject with all the needed information about the data processing purpose and the protection of medical data. The interesting point in the form is that it differs for an individual benefiting from an individual plan and an individual benefiting from a company plan. This second category of beneficiary has the option to authorise an additional level of access covering health and medical information. The BUPA consent form thus gives access to different pockets of information.

Consent to support social care assistance

Clinica Virgen Blanca

Website: https://www.clivb.com/
URL: https://clivb.com/pdf/LOPD-IM-010-protecciondatos.pdf

Description: This consent form drafted by a private medical practice contains a clear explanation of the general information on personal data protection before asking the patient his/her consent to share his/her medical data with his/her insurance and with his/her relatives.

Good Practices: The plus point of this short document is that it gives different options to the patient (to consent or not to consent) for each case.

Multiple choice consent forms

Pita Lopez Fundacion
Website: www.fundacionpitalopez.es
URL: http://fundacionpitalopez.es/wp-content/uploads/2013/03/CONSENTIMIENTO-CESION-DATOS.pdf

Description: The general consent form drafted by the Pita Lopez Fundacion allows it to collect and process a wide range of personal data from patients with cerebral damages.

Good Practices: While it it may be seen as a good use of patient time to use one form for several types of data processing consent, it is important that the form is not too general. Where a form seeks to obtain consent to a wide range of personal data processing purposes, it is questionable if this form would comply with the GDPR.

Consent in the context of medical fees reimbursement

InterGlobal – International Private Medical Insurance

Website: https://interglobal.aetnainternational.com
URL: https://interglobal.aetnainternational.com/wp-content/uploads/2014/04/UK-FCA-Medical-Claim-Form-Spanish-M001-58S-010114.pdf

Description: This consent form drafted by the International Private Medical Insurance seeks the patient consent on the processing of medical data in order for him/he to obtain the reimbursement of his/her medical costs.

Good Practices: The form is very comprehensive. However, it may be deemed too complex. The form is a spans five pages, many to which have very small type face sections.