Proceedings of the 2012 IEEE 12th International Conference on Bioinformatics & Bioengineering (BIBE), Larnaca, Cyprus, 11-13 November 2012

Security Issues in research projects with patient`s medical data

Nikolaus Forgó, Magdalena Góralczyk, Constantin Graf von Rex
Institute for Legal Informatics
LUH Hannover, Germany
forgo@iri.uni-hannover.de
goralczyk@iri.uni-hannover.de
constantin.rex@iri.uni-hannover.de

Abstract— **The article presents the possible security issues in a European research project concerning medical data with reference to the specific project Linked2Safety. A distinction is made between legal and ethical requirements for such a research project.**

Keywords - Security, clinical tirals, patients, medical data (key words)

I. INTRODUCTION

As part of a European research project, which is dealing with medical data of patients there are some security issues that must be considered and resolved because of the legal and ethical requirements. On the one hand the European and respective national legislation, set the framework for such a research project. On the other hand, the limitations of such a project derive from ethical principles, which partly overlap with the legal requirements. When patients take part in a medical research project their data and particularly their health data are being used, this might have an impact on the safety and autonomy of patients Therefore a security framework needs to be developed, which will consider both: legal and ethical risks and will safeguard the patient/ research interests in the project.

After a brief presentation of the project Linked2Safety (II.) the legal (III.) and ethical requirements (IV.) will be presented. On the last step conclusions are drawn (V.).

II. PRESENTATION OF THE PROJECT LINKED2SAFETY

The project, which will be considered by way of example is Linked2Safety. This is a project funded by the European Commission under the area of ICT for health. The aim of the project is the acceleration of medical research and support of clinical practice. This shall be achieved by a platform on which the users will receive efficient and homogenized access to distributed Electronic Health Records (EHR). The reuse of EHRs in clinical research should also be improved by the project. Within the project all legal and ethical problems will be investigated with a special focus on the requirements of the European data protection law. A Linked2Safety Data Privacy Framework will assure the compliance with the European and national legislation on data protection, with regard to publication, access and reuse of patients' personal and healthcare data.

III. LEGAL REQUIREMENTS

Whenever processing medical data, research projects, among them Linked2Safety need to consider and fulfill special legal requirements for data processing.

A. Personal and non personal data

When assessing the legal requirements for a security framework within research projects differentiation has to be made between personal and non-personal data. Personal data is understood as those data that leads to an identified or identifiable subject. Data that does not lead to an identifiable subject because of its aggregation or anonymization is therefore non-personal. The data is aggregated when those components of a record are removed and put together that make the data comparable to other records. Anonymization of the data suggests that all the elements are taken from the data which create a relationship to a living person. Every identifying chracteristics shall be deleted. From the legal point of view the difference between aggregated and anonymized data has no consequences. Both are non-personal data and therefore not within the scope of data protection rules.

At European level the principles for the protection of personal data are defined by the Data Protection Directive (DP-Directive) [1]. The EU Directives do not apply directly in the EU member states but have to be transposed into the national legal systems, hence next to the DP- Directive also the national data protection legislations have to be considered. The DP- Directive should ensure a minimum standard in terms of data protection in the member states. The free and secure exchange of personal data shall support proper functioning of the internal market. Although the DP-Directive is likely to be replaced by a Regulation on the data protection [2], draft of which was introduced in January this year [3], the provisions of the Directive and the implementations by the Member States are still binding.

978-1-4673-4358-9/12/$31.00 ©2012 IEEE

DP-Directive applies only to processing of personal data. The DP-Directive defines personal data as [Art 2 (a)]:

"any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity"[1],

Whenever data has no personal reference the principles of the DP-Directive do not apply.

Important for an EU project that is based on data from real patients, is that the data will also be personal data if the controller is not in the position to identify the patient as the data subject but somebody else, a third party, is able to do so with reasonable means.. Identifiable in this context means any information which has reference to a concrete living person.

Data is therefore personal data if the risk of re-identification is real and not merely theoretical.

Once medical data of patients is included in a research project, these types of data are sensitive personal data. For these special data the DP Directive forces the EU member states to increase the protection for it. According to art.8 para.1 DP-Directive the health data fall under the category of sensitive data which should be protected in a special way.

B. Data controller and data processor

An important distinction that plays a profound role for the security measures is to distinguish and differentiate between the data controller and the data processor. The latter process personal data for a controller and therefore they have to fulfill particular duties and responsibilities.

In the case of the project Linked2Safety the data controllers are the partners of the project, who have collected all the personal data.

According to art.2 lit.d of the DP-Directive the data controller is defined as a

> "natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his/her nomination may be designated by national or Community law."

The term data processor means for art.2 lit.d of the DP-Directive a

> "natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller".

Between the data controller and the data processor a contract is concluded which usually contains liability clauses.

In general the data controller is the one who is responsible for data processing. In simple words he or she has to make sure, that the whole process of processing the personal data is compliant with the data protection laws. According to art.6 para.2 of the DP-Directive the data controller has to ensure that data quality principles are complied with. The implementation of appropriate and necessary technical and organizational measures is up to art.17 of the DP-Directive also the duty of the data controller.

Pursuant to art.10 and art.11 of the DP-directive it is required to reveal the identity of the data controller and the identity of its representative. This is not least necessary if liability cases appear.

If within the framework of the data processing requirements of the DP- Directive are violated, the data controller is obliged to compensate for any damages a person suffers from the breach of the DP-Directive. The data controller is not liable if he is able to prove that he is not responsible for the event giving rise to the damage.

Other duties of the data controller, for example in relation to information, the data controller has to give to the respective data subject are to be found in art.10 to art.14 of the DP-Directive.

C. Pseudonymisation and anonymisation of data

Although within the DP-directive the term pseudonymous data is not used, the way of pseudonymisation of data is considered as a safety measure in research projects[4].

In the German Federal Data Protection Act in article 6 para.3 a definition for the pseudonymisation of data can be found:

> "replacing a person's name and other identifying characteristics with a label, in order to preclude identification of the data subject or to render such identification substantially difficult".

If it is possible to recode the data so that the data subject can be reidentified, it is called pseudonymous data. The possibility to reidentify the data subject is an advantage of pseudonymous data. In the case of pseudonymous data the person behind the data can be identified with acceptable effort and therefore the general data protection rules are to be applied to pseudonymous data. Under typical pseudonymisation a third party cannot determine from the pseudonymous data the patient. Consequently, patient confidentiality would not be violated even if this data were known to any unauthorized third party. The data management is simplified thereby considerably, because it will be less costly technical and organizational measures required.

As the highest safety measure in research projects with medical data of real patients, the anonymisation of data is considered [4]. According to the DP-Directive data are then anonymous, if the person standing behind the data cannot be identified with reasonable means (in terms of costs, effort and manpower) [1].

However it has to be considered that the anonymisation of data also represents a form of data processing, because Art.1 para.2b of the DP-Directice defines the processing of personal data as

> "any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction".

This definition covers any operation performed on personal data, thus also the anonymisation of data.

The anonymisation of personal data is therefore a process that falls under the same rules like any other form of processing.

The DP-Directive provides rules for the fair and lawful processing of personal data, which must be observed for the anonymisation of data, as much as for any other kind of processing.

The principle of legitimacy demands that without a legal basis any processing of data is not allowed. In addition the principle of purpose limitation limits the processing of personal data. First the data have to be collected explicitly for a legitimate purpose. Any further processing of the data is only allowed if it is consistent with the original purpose. For a research project like Linked2Safety, this means that data collected for another research project shall not be allowed to be processed automatically in the project also Linked2Safety. For such data to be processed in a project like Linked2Safety a foundation of legitimacy as the explicit consent of each affected patients for the future use of their data in research projects is required.

The DP-Directive itself provides for research with personal data another legal basis for the processing of personal data here. Because the Member States can provide appropriate safeguards and then further processing of data for historical, statistical or scientific purposes is allowed. Member states can provide in their national laws, the possibility that data will be used in future medical research projects without each of the affected patient expressly consenting to such a future use of its data. Unless member states have made use of this facility, it is not possible for example for hospitals, to use patient data for future research projects. At the same time the weakness of the DP-Directive occurs, because it is not exactly defined what is meant by appropriate safeguards.

Examples of appropriate safeguards, can be called strict data access rules and regulations for accurate pseudonymisation of data.

The possibility to use patient`s health data for the purposes of medical research depends on national law which may allow such a use.

The principle of proportionality requires that personal data that is processed must be adequate, relevant and not excessive in relation to the purposes for which these are collected and further processed.

Data shall be accurate and where necessary, kept up to date. Finally, data should also be kept in a form which permits identification of the patients behind the data for no longer than it is necessary for the purposes for which the data were collected and are further processed. Again the DP-Directive provides that member states have an obligation to lay down appropriate safeguards for the data stored for longer periods for historical, statistical or scientific reuse in future.

Art.7 of the DP-Directive lists specific cases in which processing of data is not prohibited. Thereafter the processing of data is permitted, if the person, whose data shall be processed, has given his/her consent to do so, or the processing is necessary to fulfill an obligation or the processing is in the patient`s interest.

Processing is in third party or public legitimate interest and this interest is not overridden by the data subject's interest [1].

A more strict data protection regime is provided for sensitive data like health records of patients, the Directive provides conditions under which these data can be processed in art. 8.

Art.8 para.2 of the DP-Directive clarifies that the generally prohibited processing of personal data is allowed if the patient behind the data has given his or her consent to do so. In addition the processing of such data is permitted, if the processing is necessary for the purposes in the field of employment law or to protect the interests of the patients. Additionally the processing of sensitive data can be allowed, if processing is carried out in the course of its legitimate activities with appropriate guarantees by a foundation, association or any other non-profit-seeking body with a political, philosophical, religious or trade-union aim. Finally the processing is not prohibited if the processing relates to data which are manifestly made public by the data subject; or it is necessary for the establishment, exercise or defence of legal claims.

D. Informed consent

As just described, the informed consent of a patient is one of several ways to legitimize the processing of patient data.

Regarding the informed consent of patients to participate in clinical research and in respect of the informed consent of patients to process their data, especially their health data, there are similarities and differences.

The consent to participate in a medical research project means a decision of the individual patient. As an indication of desire on the other hand, the consent of patients to process their own data is considered. Already thereto can be seen that the consent to participate in a research project is focusing on

the decision process and the consent for data processing is more or less only the notification of the decision.

A special feature in terms of the consent for processing patient`s data is that there is a difference between the one for personal data and for sensitive data, such as health data. Consent for processing personal data must be made clear by the patient. The consent for the processing of sensitive data must be explicitly given by the patient. An explicit consent cannot be implied. The patient must actively and explicitly opt for the processing of sensitive data.

For a research project like Linked2Safety a possibility may be considered that would allow the processing of patient data without their consent. In art.8 para.4 of the DP-Directive it is stipulated, that subject to adequate provision of guarantees by the member states, these are given the opportunity, if an important public interest requires so, to provide exceptions to the general prohibition on processing sensitive data through a law or decision of the supervisory authority. Recital 34 of the DP-Directive can be found that medical research can be understood as such an important public interest. In the Cypriot data protection law may be found for example that it is allowed to use health data for research purposes on condition that all necessary measures are taken for the protection of the data subject [5].

E. Technical and organizational measures

To ensure the security of the data, technical and organizational measures have to be taken.

Pursuant to art.17 para.1 and 2 of the DP-Directive, member states shall provide that

> "the controller as well as processor must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing."

Through measures such as these the data should be protected. If a case of so-called commissioned data processing is present, which means that data are processed in the name of the data controller by the data processor, the whole process of data processing must be governed by a contract or legal act which entails the obligations of the data processor. The DP-Directive does not give further detailed information regarding the design of the technical and organizational measures.

The Council of Europe Committee of Ministers helping member states with section 9 of the Recommendation No. R (97) 5 on the protection of medical data [6]. Such a Recommendation has no legally binding effect, but member states are encouraged to implement the contents of such recommendations in their national laws.

Particular recommendations with regard to appropriate technical and organizational measures include the need for measures:

- to prevent any unauthorised person from having access to installations used for processing personal data (control of the entrance to installations);
- to prevent data media from being read, copied, altered or removed by unauthorised persons (control of data media);
- to prevent the unauthorised entry of data into the information system, and any unauthorised consultation, modification or deletion of processed personal data (memory control);
- to prevent automated data processing systems from being used by unauthorised persons by means of data transmission equipment (control of utilisation);
- with a view to, on the one hand, selective access to data and, on the other hand, the security of the medical data, to ensure that the processing as a general rule is so designed as to enable the separation of identifiers and data relating to the identity of persons, administrative data, medical data, social data and genetic data (access control);
- to guarantee the possibility of checking and ascertaining to which persons or bodies personal data can be communicated by data transmission equipment (control of communication);
- to guarantee that it is possible to check and establish a posterior who has had access to the system and what personal data have been introduced into the information system, when and by whom (control of data introduction);
- to prevent the unauthorised reading, copying, alteration or deletion of personal data during the communication of personal data and the transport of data media (control of transport);
- to safeguard data by making security copies (availability control).

In addition, those who are responsible for the processing of medical data, shall name a competent person for the information security and privacy, to provide information on the above mentioned recommendations.

Neither in the DP-Directive nor in the Recommendations of the Council of Europe Committee of Ministers can be found exactly what steps to take in terms of data security technology. Instead the DP-Directive and the Recommendation give more general information. This procedure is explained by the fact that technological progress is subject to constant change and

therefore no techniques may be required or recommended. It is up to the data controller to install a security system which fulfills the general requirements for data security and privacy. Furthermore, it is the duty of data controller to ensure that this security system is always renewed subject to the technical development progresses. When choosing a security system there are many factors that have to be considered, such as the risks of the data processing, the nature of the data, as well as costs of their implementation. As regards Linked2Safety the required security standards have to be high because the project deals with medical patient data which are considered to have sensitive character and at the same time a lot of people might have access to it.

A generally accepted information security standard is for example "ISO/IEC 27001:2005 Information technology – Security techniques – Information security management systems" [7] which specifies requirements for the establishment, implementation, monitoring and review, maintenance and improvement of a management system for managing an organisation's information security risks [9].

F. Rights of the data subject

Among the security measures in a research project that deals with medical records must include the rights of the individual data subjects/ the patients, that must be observed.

From the DP-Directive result the individual rights of patients as data subjects, which are described in detail the following:

- right to be informed;
- right of access;
- right of rectification, erasure or blocking; and
- right to object.

To describe in detail exactly the rights of the patients as data subjects is beyond the scope of this abstract, but it can be summarized for the safety measures that the data controller has to observe the patients' rights and always has to allow the exercise of their rights arising from the DP-Directive.

For a research project like Linked2Safety, which is based on sensitive data, there are as above mentioned, different legal requirements that must be taken into consideration.

G. Transfer of personal data to third countries

Another security issue may be the transfer of patient`s personal data to any country outside the European Union and / or the European Economic Area. Such a transfer is only allowed if a European-standard level of data protection. is guaranteed, Articles 28 and 29 of the DP-Directive.

In the case of Linked2Safety the personal data is processed anonymously so that no problems should arise during the transfer to third countries though.

IV. ETHICAL REQUIREMENTS

In addition to legal norms medical research projects must also comply with ethical requirements whatsoever. The example project Linked2Safety has therefore stated its objective to respect the rights of the participating patients and the legal and ethical requirements in the European Union.

A special feature of this project is that no personal data is processed on the platform which is to be developed in the project. Rather, the collected patient data is processed and anonymised on a computer that is not connected to the infrastructure of the project. It should not be ignored, that is still within the scope of the project data to be processed, where legal and ethical requirements have to be observed.

A. Informed Consent

From the ethical perspective the patient's informed consent plays a very important role in a medical research project like Linked2Safety. The idea behind the requirement of informed consent of patients is that any medical procedure, which has an impact on the patient requires his/her prior written consent based on comprehensive information. The patient can freely decide whether he or she wants to take part in the research project after he/she received enough and understandable information about what is planned in the project. In that way the fundamental rights of self determination and dignity are protected.

For the project Linked2Safety the Declaration of Helsinki – Ethical Principles for Medical Research Involving Human Subjects ("Declaration of Helsinki") [8] which was adopted by the World Medical Organization ("WMA") serves as an ethical guideline.

So that the informed consent meets the ethical standards of the Declaration of Helsinki, the individual patient has to be informed in an appropriate manner and consent must be given voluntarily. In addition the individual patient must be able to come to a decision like the consent or he must have a legal representative who can take this decision for him. Furthermore the consent should be in writing.

Both the content of the information and the way of their presentation to the patient must be such that patients are not overwhelmed and understand as much as possible.

In addition patients have to give their informed consent voluntarily and freely without any external pressure to do so.

To guarantee patient`s right of self-determination the patient asked to give his or her informed consent should be capable to take the decision to participate or not in a medical research project [8].

If the respective patient is not able to give his informed consent to participate in the medical research project, the consent should be obtained from the legally authorized representative [8].

The patient should have the right to withdraw his or her consent to take part in a medical research project at any time.

Both the informed consent and the withdrawal should be in writing [8].

In the case of the project Linked2Safety, where the consent to the collection, processing and use of health data is needed, it should always be a possibility to revoke the once given consent [8].

The question of the scope of the patient`s informed consent is beyond the scope of this essay, however, that reference is allowed, that with respect to the project Linked2Safety the so called broad or blanket consent would be the best solution. The specified consent cannot be implemented as part of the project, because the future projects that will build on L2S are not yet known. The tiered consent has considerable administrative side effects. Ultimately it is the decision of the responsible entity for which type of consent they choose.

B. Other ethical requirements

When it is not possible to obtain patient`s consent or at least the consent from the patient´s legally authorized representative it is questionable how to proceed in the relevant research project. A solution to this problem could be to render the personal data anonymous. After the data is rendered anonymous it requires considerable effort to identify the person behind the anonymous data. Because it requires large expenditure to reanonymise the anonymised data sovereignty of the patient`s data is not hurt by the processing of the data and the ethical requirements are observed. The project Linked2Safety is processing anonymous data only, so the problem of missing patient`s consent is solved.

Another ethical requirement for a medical research project is that the methods used "must conform to generally accepted scientific principles, be based on a thorough knowledge of scientific literature, other relevant sources of information and adequate laboratory" [10] Furthermore a research project like Linked2Safety has to be lead and monitored by qualified and trained persons only [9].

V. CONCLUSION

Personal data and especially sensitive data needs special protection in a research project which deals with patient`s medical data. Once there is non-personal data involved the European and national data protection laws do not apply.

One way to protect the personal and sensitive data from patients in particular is making the data anonymous. Personal patient data are therefore processed in an anonymous form only in the project Linked2Safety.

The safety and privacy of patients' data must be ensured by the data controller. In the case of a medical research project is responsible for personal data the data controller, as the one that collected the data from the patient. In the case of the research project Linked2Safety the data controllers are the clinical partners of the project.The data controller and the data processor have different duties to fulfill. If a data protection subject suffered a loss of a violation of the requirements of the DP-Directive the data controller has to compensate for this damage.

The DP-Directive provides technical and organizational measures to guarantee the protection of the personal data. The informed consent of patients is one of the demands made by both ethical and legal side of a research project and must therefore be mindful of the security issues as well. In addition, the rights of data subjects have to be respected, as well as the conditions for the transfer of data to third countries, if such scenarios come up.

ACKNOWLEDGMENT

The work is part of the on-going Linked2Safety-project (grant agreement n°288328) funded under the FP7 framework of the European Union. The content of this article reflects the views of the authors and not necessarily that of the project consortium.

REFERENCES

[1] See Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data, (24.10.1995).

[2] See Commission Proposal for a Regulation of the European Parliament and of the Council, COM (2012), 11 final (25.01.2012).

[3] N. Stolba, A.M. Toja, An approach towards the fulfilment of security requirements for decision support systems in the field of evidence-based healthcare, www.citeseerx.ist.psu.de, 2006.

[4] Article 29 Data protection working party, Opinion 4/2007 on the concept of personal data, 2007.

[5] www.dataprotection.gov.cy/dataprotection/dataprotection.nsf.

[6] https://wcd.coe.int/com.instranet.InstraServlet.

[7] http://www.iso.org/iso/catalogue_detail?csnumber=42103.

[8] www.wma.net/en/30publications/10policies/b3/.

[9] J. Pedroni, K. Pimple, A Brief Introduction to Informed Consent in Research with Human Subjects, The Trustees of Indiana University, 2001, p.4.

[10] N. Forgó, R. Kollek, M. Arning, T. Kruegel, I. Petersen , Ethical and Legal Requirements for Translational Genetic Research, C.H. Beck: München, 2010.