Measuring quality of care in the treatment of acute coronary syndrome

Eindhoven, D.C.

Chapter 8

Privacy of patient data in quality-of-care registries in cardiology and cardiothoracic surgery

The impact of the new General Data Protection Regulation EU-law

E. Wierda, MD[1], LLM, D.C. Eindhoven, MD[2], A. Hirsch, MD, PhD[3], M.J. Schalij, MD, PhD[2], C.J.W. Borleffs, MD, PhD[4], G. Amoroso, MD[5], D. van Veghel[6], B.A.J.M. de Mol, MD[7], M.C. Ploem, LLM[8]

E. Wierda and D.C. Eindhoven contributed equally to this article and therefore share first authorship.

1. Department of Cardiology, Academic Medical Center, Amsterdam
2. Department of Cardiology, Leiden University Medical Center, Leiden
3. Department of Cardiology and Radiology, Erasmus University, Rotterdam
4. Department of Cardiology, Haga ziekenhuis, Den Haag, The Netherlands
5. Department of Cardiology, Onze Lieve Vrouwe Gasthuis, Amsterdam
6. Department of Cardiology and Cardiothoracic Surgery, Catharina Hospital, Eindhoven
7. Department of Cardiothoracic Surgery, Academic Medical Center, Amsterdam
8. Department of Social Medicine, section Health Law, Academic Medical Center, Amsterdam

Published: Eur Heart J Qual Care Clin Outcomes. 2018 Oct 1;4:239-245

ABSTRACT

Aims

Quality-of-care registries have shown to improve quality of healthcare and should be facilitated and stimulated. The data of these registries are potentially also very valuable for medical data research. While fully acknowledging the importance of re-using already available data for research purposes, concerns about how the applicable privacy legislation is dealt with exist.

Legal framework

In Europe, the new EU law on privacy, the 'General Data Protection Regulation' (GDPR) will come into force on May 25th 2018. One of the main rules is that non-anonymous patient data may, in principle, not be used for research without the patient's informed consent. When patient data are solely and strictly used for quality control and improvement this rule does not apply. It is especially important that registries take into account applicable privacy legislation because the GDPR makes it possible for national supervisory authorities to impose high fines to institutions in case of violation.

Implications

In this study we provide examples of quality-of-care registries in the field of cardiology and cardiothoracic surgery in Europe. None of the described registries (NHR, SWEDEHEART and MINAP) currently ask specific informed consent of patients before using their data for medical data research. In order to comply with the new European data protection rules the advice to healthcare institutions is therefore to explicitly inform patients about the possible use of their data for quality-of-care registries while also designing a proper informed consent procedure to facilitate and optimize the use of quality-of-care data for medical data research.

INTRODUCTION

Privacy and confidentiality are core principles of a safe patient-physician relationship. Over a lifetime, important information about medical history, medication use, diagnostic tests and therapies is registered in patients' medical records. Medical information is considered to be a special category of data, as for most patients the disclosure of the fact that a person suffers from progressive heart failure, a psychiatric disorder or cancer is a far more sensitive aspect of their personal life than for instance the make of car they drive.[1] While in the past, data used to be registered and stored in the form of paper records, nowadays data is digitally collected and stored in Electronic Patient Records (EPRs) and easy accessible. Healthcare institutions handle large amounts of digital patient data in such records.[2]

Consequently data from EPRs are collected in centralized national quality-of-care registries.[3] These data are very useful for secondary purposes, such as the monitoring of outcome measurements of hospitals and medical data research. The digital revolution and subsequent improvements in ICT have made it possible to collect and analyse large amounts of medical data.[4, 5] The current availability of collected volume (with linking possibilities), velocity (real-time data) and variety (claim and clinical data) of data, leads to data becoming 'big data'.[6] 'Big data' by definition refers to electronic health datasets so large and complex that they are difficult to manage with traditional soft- and hardware, nor can they be easily managed with traditional or common data management tools.[3] By comparing and analysing 'big data' sets, it is hypothesized that efficiency and quality of healthcare may be improved and potentially at lower costs.

Privacy and data protection are an important and ongoing concern. Recently, multiple healthcare organizations in the United States have been the target of hackers stealing personal patient data with more than 1 million patients affected.[7] Furthermore, in 2016 Hospital Trusts within the National Health Service (NHS) in England and Scotland were hit by a large ransomware attack, which resulted in locking computers and demands for payment for them to be unlocked.[8] A different and perhaps more serious problem is that many medical organizations do not appear to be fully aware of the relevant legislation and the implications of using patient data for secondary purposes as monitoring of quality and medical data research.[9] This not only create risks for healthcare professionals and institutions - varying from reputational damage to financial loss due to the high relating fines[10] - but it may also have a negative impact on the patient-physician relationship.

In this study, first a few examples of quality-of-care registries in the field of cardiology and cardiothoracic surgery will be given. Next, a general overview of the European and Dutch legal framework (relevant data protection and privacy legislation) applying to quality-of-

care registries is provided. Finally, the specific implications of these laws and regulations for quality-of-care registries, what level of privacy protection is required, the potential problems in this regard and possible solutions are discussed. With respect to the latter, this article focuses on the future of these registries and make some recommendations.

QUALITY OF CARE REGISTRIES IN CARDIOLOGY AND CARDIOTHORACIC SURGERY

A quality-of-care registry is usually an independent organization maintaining a database containing information about a patient population with a specific disease, type of care or complication or a combination of these, that is used to measure, improve and report the quality of the care provided. The registry also organizes the processes to select and define the parameters. Monitoring quality of care primarily involves collecting and analysing and publishing specific patient data and results of the care delivered. Describing these in comparable patients using pre-specified variables, relationships and comparisons gives insight into how to improve the quality of care.[11] Healthcare providers collect data by entering data into a portal, by automatically linking electronic patient records or by delivering files with data. In most countries, 'raw' medical data cannot be owned, however health care providers have responsibilities towards patient data concerning certain patient rights, such as the patient's right to medical confidentiality.

After the data collection phase, the data files are securely stored after being encrypted by the registry. Subsequently, these aggregated data are analysed and adjusted by the agency that is responsible for the registration, then prepared for publication. The results are reported back to the healthcare providers themselves but also to the public and to other specific stakeholders, such as healthcare insurance companies, regulatory agencies and patient's groups. When combining different databases, a third trusted party acts as an intermediary who links encrypted data with personal identifiable data (e.g. date of birth). To ensure the quality of the data analysis, registries comply to international standard frameworks for information security, such as NEN 7510 (for securing of data), 7512 (for exchanging data) and 7513 (for logging and access to data).[12]

Three national quality registries in cardiology and cardiothoracic surgery in the Netherlands, Sweden and United Kingdom will be described. For each registry will be discussed how they handle privacy and informed consent issues. An overview is provided in **Table 1**.

National Registries in Cardiology – The Netherlands

The Netherlands Heart Registration (Nederlandse Hart Registratie, NHR) is the major cardiovascular quality-of-care registry in the Netherlands.[13] The registriy was initiated by healthcare professionals involved and funded by participating departments.[14] Outcome indicators for cardiothoracic surgery, acute coronary syndromes, percutaneous coronary intervention, transcatheter heart valve implantations, ablation of atrial fibrillations and device implantations are included. The aim of the NHR is to improve quality of care by reporting outcome indicators in yearly publicly accessible reports. The NHR has a NEN-7510 certification. Encryption is used to pseudomize personal data.[15, 16] Participating hospitals are responsible for data collection and registration and remain the owners of these data.[17]

National Registries in Cardiology – Sweden

Swedish Web-system for Enhancement and Development of Evidence-based care in Heart disease Evaluated According to Recommended Therapies (SWEDEHEART) is a Swedish quality-of-care registry in Sweden that reports the outcome of hospitalised patients with respect to acute coronary syndrome and coronary or valvular intervention.[18] Every hospital in Sweden takes part in the registry which is publicly funded. A personal identity number is used by healthcare authorities in medical records. All quality registries are regulated by the Swedish Patient Data Act (2008:355).[19] According to this act, caregivers are allowed to use personal data entered in a registry for the primary purpose of developing and securing the quality of care. Before personal data are entered in a registry, the responsible authority has to inform the patient. The patient may oppose registration, but the law does not impose a requirement of any (signed) consent from the individual.[20]

National Registries in Cardiology – Great Britain

In the United Kingdom, Myocardial Ischaemia National Audit Project (MINAP) is the quality-of-care registry for myocardial infarction that collects the outcomes of patients in England, Wales and Northern Ireland. MINAP was started in 2000 and all 230 acute care hospitals in these regions participate in the registry. More than 1.300.000 patient records have been included. MINAP never publishes information that could lead to identification of individual patients, because patient records are cleaned and anonymised. Informed consent is not asked. MINAP conforms to legislation within the relevant Data Protection Act for the collection and use of patient identifiable data. Section 251 of the NHS Act 2006 allows the common law duty of confidentiality to be set aside in specific circumstances where patient consent is not attainable.

In summary, although the specifics of the saved personal data and omission of identifiable data differ somewhat between these three described European registries, they all secure data by encoding and use so-called Privacy Enhancing Techniques. None of the registries

ask the patient for informed consent to use their data in the quality-of-care registry. All of these registries carry out medical data research using the collected patient data.

LEGAL FRAMEWORK

Requirements following from international and European regulations

Quality-of-care registries collect and process large amounts of patient data, not only to use them for monitoring simply the quality of care within a single institution, but also to improve quality of healthcare (amongst others by publishing data analyses) and to stimulate medical data research. To facilitate this type of research, long-term storage and data linkage are prerequisites.[21] The latter is significant because the legal provisions applying to setting up and using patient data purely for quality monitoring and the provisions for carrying out medical data research (and setting up research databases) are not the same.

The main rules concerning patient data are provided by binding legislation from the European Union (EU). From 1995 until 2018, the governing EU legislation was the European Privacy Directive (Directive 95/46/EC) on processing of personal data.[22] In 2012, the European Commission of the EU proposed a comprehensive reform of the EU's privacy directive. A strong and more coherent data protection framework in the EU seemed necessary in light of rapid technological developments and globalisation, which brought new challenges for the protection of personal data. The new EU law, the 'General Data Protection Regulation' (GDPR), was adopted in April 2016 and will come into force on May 25th 2018.[1] The GDPR does not require implementation and is directly applicable in all member states to ensure a consistent and high level of protection of individuals. The GDPR makes it possible for national supervisory authorities to impose high fines to institutions in case of violation.

The leading principle of the GPDR, as included in article 9, is that the processing of personal data is prohibited, but it is allowed in specific cases set out in the GDPR. Proving explicit informed consent is an example of such an exception as well as data processing for health care purposes.

When patient data are used for monitoring quality of care within healthcare institutions, article 9, paragraph 2 sub i of the GPDR is applicable. It allows collection and use of personal data to manage healthcare systems or to guarantee high standards of quality of care.[23]

However, if quality-of-care data are used for medical data research, a stricter legal regime for the processing of the collected data should be taken into account. The main rules

are provided by the same binding legislation from the EU,[24] the GDPR. From article 9, paragraph 2 sub j GDPR follows that collection and use of personal data for medical data research is allowed when this is done in accordance with the principle of proportionality and the purpose of the research while appropriate measures have been taken to protect the rights of the individual subjects.[23] Appropriate measures include collecting the smallest amount of data necessary for research and the anonymisation of data when possible. An overview of the most important consequences of the GDPR for healthcare organisations and quality-of-care registries is provided in **Table 2**.

Because EU-law offers a general legal framework and does not specifically address medical data research, non-binding rules developed by the Council of Europe and the European Science Foundation could provide further guidance. The main principles are that non-anonymous or identifiable medical data may only be collected and analysed, if this is necessary for carrying out the research and if the data subjects have given their informed consent. However, where it would be unrealistic to seek the individual's consent, personal data may still be collected and used, provided that certain conditions are met. One of these conditions is that the patient knows about the possible use of his or her data for medical data research (right to be informed on a general level) and has not objected to this (right to opt out).[25]

Requirements following from Dutch law

In the Netherlands, according to the Dutch law on Quality, Complaints and Disputes in Healthcare (*Wet kwaliteit, klachten en geschillen zorg*),[26] it is considered an obligation of each healthcare institution to collect and register quality-of-care patient data and to use these for monitoring, assessing and improving the quality of the care provided to patients. The latter law contains no specific requirements on the protection of patient data. As mentioned before, in the Dutch cardiovascular quality-of-care registry (NHR) participating hospitals are responsible for data collection and registration and remain the owners of these data.[17]

Compared to the number of scientific publications from the Swedish and British registry, the Dutch cardiovascular registry only published a few papers in scientific journals with data published in yearly reports before. When quality-of-care data are used for medical data research purposes, apart from the GDPR and its additional provisions on a national level, the Medical Treatment Contract Act (*Wet op Geneeskundige Behandelovereenkomst*, referred to as WGBO, a section of the Dutch Civil Code) is particularly relevant because this law contains specific rules on data processing for medical data research. The main requirement is patient consent (Article 7:457 Civil Code). However, when it is reasonably not possible (patient is deceased or untraceable) or feasible (large amount of patients, large chance of

non-respons) to obtain consent the requirement for consent may be put aside. Then, data may only be collected from patient records if they have been pseudonymized in advance. In the event of a 'consent-waiver', three additional conditions need to be met. First, the research project should serve a public interest. Second, the research could not be carried out without the data concerned. Third, the data subject is informed about the possible use of data for research projects and has not explicitly opposed to this.

In the Netherlands, the Data Protection Authority (*Autoriteit Persoonsgegevens*) is the national supervisory authority on the processing of personal data by healthcare institutions.[27] The Dutch DPA can, similar to other EU supervisory agencies, impose high fines if the law and its legal requirements are violated.

IMPLICATIONS FOR QUALITY-OF-CARE REGISTRIES

Quality-of-care registries collect and process large amounts of patient data. The registries in the field of cardiology and cardiothoracic surgery described before not only use patient data for monitoring simply the quality of care within a single institution, but also to improve quality of healthcare (amongst others by publishing data analyses) and to stimulate medical data research.

As pointed out before, the rules for using data for medical data research are stricter than for purely quality monitoring. In most jurisdictions, based on the GDPR, one of the most important difference between to the two legal regimes is that patients have control over the use of their data for medical data research – in the form of an opt-in or opt-out possibility – while this position is absent in the context of data processing for quality of care monitoring. According to Dutch law, the basic requirement in this respect is that informed consent of patients should be obtained for using their data for research, although the law leaves room for exceptions if research would become impossible or infeasible.

Another 'escape' from the stricter rules for using medical data for research would be to collect and use truly anonymous data, because in that situation data protection and privacy legislation do not apply. Anonymised data is no longer considered personal data in the context of the GDPR and the national data protection legislation and handling those data is considered not to interfere with the privacy of the participating patients.[28] Registry data could only be considered truly anonymous if disproportionate effort is required to link the data to identifiable patients.

The best practices for complete anonymisation of data in clinical trials could be used for complete anonymisation of data in quality of care registries also. Data from datasets can be classified into either direct identifiers or indirect identifiers, where direct identifiers (like name and initials, adress including postal code) have a high risk of identifying a patient and indirect identifiers (like rare treatment, place of birth) could lead to identification.[29]

To anonymize a data set, it is advised in the literature to remove direct identifiers and to remove certain indirect identifiers (depending on the risk, p.e. indirect identifiers with small numbers are considered a high risk), recoding codes that identify patients with a new code and replacing date of birth (with age) and all patient related dates. Risky indirect identifiers could be modified if they are important for meaningful data analysis.[30] Whether indirect identifiers should be removed, modified or left, should be left to a relevant advisory body, either an ethics committee or appropriate national advisory body.[29]

Although in many quality-of-care registries, data are pseudonymised by using privacy enhancing techniques, the data contained in the described cardiology and cardiothoracic surgery registries are not truly anonymous and therefore do not escape from the consequences of the privacy and data protection legislation. First, some - but not all - identifiable data are omitted. For example if a 87-year patient undergoes a specific, not so frequent procedure at this age (e.g. a coronary-artery-bypass-grafting including mitral valve replacement), data could still be retrieved to this individual patient, although date of birth has been omitted in the database. Secondly, the source of the data is not deleted at the time of data collection (hospitals have even an obligation to store patient data in the electronic patient records for a fixed period of time). Since it is difficult - but with reasonable effort not impossible - to trace data back to individual patients, the data in these registries should be considered as pseudonymised and not anonymised.

CONCLUSION

It is beyond discussion that quality-of-care registries improve quality of healthcare and should be facilitated and stimulated.[14] in some countries, such as the Netherlands, this is even a legal obligation. Unless the personal data collected for and stored in these registries are completely anonymised, they fall within the scope of data protection law and regulations (the GDPR sets high standards for anonymisation and will be applicable in EU member states as of May 25th 2018). This implies that such data, in principle, may only be used for medical data research purposes after informing patients and obtaining their explicit consent. Some jurisdictions, such as the Dutch one, provide for exceptions (opt-out system) when research would be disproportionally hampered.

Proper information and consent procedures require considerable effort of healthcare institutions although IT-developments could make it increasingly more easy to implement. However, national supervisory authorities could impose high fines to institutions in case data protection and privacy regulations are not observed. Besides, by doing so, healthcare instutions invest in a trustworthy patient-physician relationship and they open new possibilities for researchers, such as the linking of international medical databases for future research. In order to comply with the new European data protection rules, embodied in the GDPR, the advice to healthcare institutions is therefore to explicitly inform patients about the possible use of their data for quality-of-care registries while also designing a proper informed consent procedure to facilitate and optimize the use of quality-of-care data for medical data research.

REFERENCE LIST

1. European Union Parliament, European Union Council. General Data Protection Regulation (EU 2016/679). 2016, p. Recitals 10 and 51 of the preamble.
2. Appari A, Johnson E. Information security and privacy in healthcare: current state of research. *IntJInternet and Enterprise Management*. 2010;6:279-314.
3. Raghupathi W, Raghupathi V. Big data analytics in healthcare: promise and potential. *Health Inf Sci Syst*. 2014;2:3.
4. Groves P, Kayyali B, Knott D, et al. The 'big data' revolution in health care, accelerating value and innovation. MCKinsey&Company, January 2013.
5. Manyika J, Chui M, Brown B, et al. Big Data: The Next Frontier for Innovation, Competition, and Productivity. USA: McKinsey Global Institute, 2011.
6. Laney D. 3D Data Management: Controlling Data Volume, Velocity, and Variety. *Gardner Group*. 2001.
7. United States Departement of Health and Human Services. Health Information Privacy www.hhs.gov/hipaa/ United States Departement of Health and Human Services; 2017. (Accessed 2017 May 23).
8. NHS. Latest guidance for NHS on protecting against cyber attack. https://digital.nhs.uk/article/1495/Latest-guidance-for-NHS-on-protecting-against-cyber-attack2017. (Accessed 2017 December 18).
9. van der Lee F, van Vianen R, Spronck J. Risico's van alle kanten. BDO zorg informatie beveiligingscan 2015.: BDO Branchegroep Zorg, 2015.
10. Croonen H. Datalek melden, anders volgt dikke boete. 2015, 12 November;N0. 46:2186-7.
11. Hutink H, Jong Ad, Hülsmann C, et al. Leidraad kwaliteitsregistraties. Zorginstituut Nederland Nictiz, 2016.
12. International Organization for Standardization (ISO). ISO/IEC 27001 - Information security management www.iso.org/iso/home/standards/management-standards/iso27001.htm2013.
13. Nederlandse Hart Registratie (NHR). www.nederlandsehartregistratie.nl, 2017 (Accessed 2017 October 25,).
14. Eindhoven DC, Wierda E, de Bruijne MC, et al. The year of transparency: measuring quality of cardiac care. *Neth Heart J*. 2015;23:457-65.
15. Begeleidingscomissie Hartinterventie Nederland (BHN). Handboek BHN Registratieproject, versie 4.0.1, 2015, January 1 www.nvtnet.nl/includes (Accessed 2017 December 18).
16. Moussa I, Hermann A, Messenger JC, et al. The NCDR CathPCI Registry: a US national perspective on care and outcomes for percutaneous coronary intervention. *Heart*. 2013;99:297-303.
17. Daeter E.J., et al. Meetbaar Beter Boek 2017 www.nederlandsehartregistratie.nl (Accessed 2017 December 18).
18. CardioPulse Articles. SWEDEHEART: Sweden's new online cardiac registry, the first of its kind. *Eur Heart J*. 2009;30:2165-73.
19. Socialdepartementet (Swedish Ministry of Health and Social Affairs). Regeringskansliets rättsdatabaser, Patientdatalag (2008:355) http://rkrattsbaser.gov.se (Accessed 2018, January 7).
20. Mattsson T. Patient safety at odds with patient privacy? The case of national and regional quality registries for incapacitated elderly in Sweden. *Faculty of Law*. Lund: Lund University, 2014.
21. Ploem MC. Gegeven voor de wetenschap. Regulering van onderzoek met gegevens, lichaamsmateriaal en biobanken. In: Engberts DP, Koster-Reidsma YM and Ploem MC. *Wetenschappelijk onderzoek in de zorg Preadvies uitgebracht voor de Vereniging voor Gezondheidsrecht, jaarvergadering 23 april 2010* Den Haag: SDU, 2010, p.117-206.
22. European Commission. Proposal for a regulation 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 (General Data Protection Regulation) http://ec.europa.eu/justice/data-protection/law/index_en.htm2012.

23. European Union Parliament, European Union Council. General Data Protection Regulation (EU 2016/679). 2016, p. Article 9, paragraph 2, sub h and j.
24. Ploem MC, Essink-Bot ML, Stronks K. Proposed EU data protection regulation is a threat to medical research. *BMJ*. 2013;346:f3534.
25. Ploem MC. Towards an appropriate privacy regime for medical data research. *Eur J Health Law*. 2006;13:41-63.
26. Dutch Government. Law Quality, Complaints and Disputes in Healthcare. www.overheid.nl/2015. (Accessed 2018 January 10).
27. Senate of the Dutch Parliament (Eerste Kamer der Staten Generaal). Parliamentary Papers 2014-2015, 33 662, nr. C. 2015, 19 May.
28. Data Protection Commissioner. Anonymisation and pseudonymisation www.dataprotection.ie/docs/Anonymisation-and-pseudonymisation (Accessed 2018 January 7).
29. Hrynaszkiewicz I, Norton ML, Vickers AJ, et al. Preparing raw clinical data for publication: guidance for journal editors, authors, and peer reviewers. *BMJ*. 2010;340:c181.
30. Tucker K, Branson J, Dilleen M, et al. Protecting patient privacy when sharing patient-level data from clinical trials. *BMC Med Res Methodol*. 2016;16;1:77.