European Journal of Human Genetics (2019) 27:211–215
https://doi.org/10.1038/s41431-018-0258-4

ARTICLE

Patients v. Myriad or the GDPR Access Right v. the EU Database Right

Jasper A. Bovenberg[1] · Mara Almeida[2,3]

Received: 11 May 2018 / Revised: 31 July 2018 / Accepted: 19 August 2018 / Published online: 27 September 2018

Abstract
In 2016, four US cancer patients legally challenged Myriad by claiming full access to all genomic information produced in the course of Myriad's testing of their risks for a variety of cancers. Asserting that Myriad's refusal to provide them with this information violated the HIPAA Privacy Rule, the patients sought a determination of a right to access all their genetic information from testing laboratories. Such access would not only serve their own care, but also enable them to share their genetic data with the scientific community which they alleged Myriad failed to do. A similar case may be brought in Europe under the novel EU GDPR. Specifically, it would put the GDPR right of access to personal data against Myriad's database right under the EU Database Right Directive. The outcome of this case could impact the fate of personalized medicine, which depends on the one hand on patients' having control over their genetic data, and on the other hand on incentives for genetic testing companies to generate these data. We first address the issue of whether the GDPR applies to medical records. We then analyse how GDPR rights could play out in the context of clinical genetic testing and conclude that the GDPR access right stops short of granting unconditional access to all data generated in the process of testing, to the extent that its exercise would result in the violation of medical-professional norms, expose the testing company to potential liability, or compromise normal exploitation of the database of which the personal data form part.

Background

In 2013, the US Supreme Court partially invalidated a number of Myriad Genetic Laboratories, Inc. (Myriad)'s patents on breast cancer genes, in a lawsuit brought by the American Civil Liberties Union (ACLU). As the patents had allowed Myriad to monopolize clinical testing of these genes and to assemble an enormous amount of information on variants of a gene associated with breast cancer (BRCA) from the patients it tested [1], Myriad could continue to base its business model on claiming proprietary control over these data, calling itself a 'genetic information business' [2, 3]. On 19 May 2016, however, this new model faced its own legal challenge, when four US patients, represented by the ACLU, submitted a complaint against Myriad with the US Department of Health and Human Services (HHS) [4]. The patients had obtained testing from Myriad to determine their hereditary risk for breast, ovarian and other cancers and to guide potential treatment options. The legal dispute was initiated when Myriad refused to provide access to the additional, underlying information it had obtained during the testing process, but not included in the test reports. Myriad considered this information not to be part of the patients' Designated Record Set (medical record), in addition to stating that part of the information had been deleted. Asserting that Myriad's refusal violated the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule, the patients sought a determination by the HHS that patients have a right to access all their genetic information from testing laboratories and adoption by Myriad of a policy providing for patients' access to their own genetic information [2]. They were not only motivated to get this information for their own and their family's benefit, but also to share their data with the broader research community

✉ Jasper A. Bovenberg
jabovenberg@xs4all.nl

✉ Mara Almeida
msalmeida@fc.ul.pt

[1] Attorney at Law | Haarlem, The Netherlands & New York, NY, USA

[2] Institute of Chemical and Biological Technology, University Nova of Lisbon, Lisbon, Portugal

[3] Present address: Centre for Philosophy of Science of the University of Lisbon, Lisbon, Portugal

and so challenge Myriad's business model based on its exclusive control over these data [3].

While, to the best of our knowledge, the HHS's investigation is either still pending or has been settled, a similar complaint is likely to be brought before a European court, as patients may want to try to apply the novel European Union (EU) General Data Protection Regulation (GDPR) to genetic testing. The GDPR will apply to any organization that processes any EU personal data regardless of where it is located around the globe and offers citizens the right to access their personal data, the right to obtain a copy of their personal data and the right to transmit their personal data to a third party [5]. The outcome of such a case will impact the advent of personalized medicine, which depends on patients' having control over their data on the one hand and on incentives to generate diagnostic data on the other hand. Indeed, the issue is of relevance for all research processing personal data, in science and industry.

Does the GDPR apply to medical records?

If EU patients were to claim, as the US patients did, that all genetic data produced by Myriad forms part of their medical record, then a preliminary, if mandatory issue must be answered, i.e., whether the GDPR applies to medical records in the first place. Privacy and data protection are fundamental rights according to the EU Charter of Fundamental Rights [6]. Article 1 [2] of the GDPR aims to protect in particular the right to data protection. That does not mean, however, that all processing activities fall under the scope of the GDPR. The scope of the GDPR is laid down in article 2 which, inter alia, explicitly states that the GDPR does not apply to activities which fall outside the scope of Union law. That raises the question of whether processing in the context of medical care is within or without the scope of Union law. As a piece of EU legislation, the GDPR must be compatible with the EU Treaty under the principle that legislative competence not conferred upon the EU remains with the Member States. This requirement seems to be met as the GDPR is based on Article 16 [1] of the Treaty, which provides that everyone has the right to the protection of their personal data. However, the Treaty also provides that the delivery of medical care is the exclusive responsibility of the Member States. Since the medical record is a mandatory part of the delivery of care, it could be argued that, since the EU has no competence over the practice of medicine, the application of the GDPR to medical records infringes the EU Treaty [7]. In addition, it could be argued that the application of the GDPR to medical records would violate the EU Treaty principle of subsidiarity—which aims to 'ensure that decisions are taken as closely as possible to the citizens of the Union'.Member States have doctor–patient confidentiality regimes in place which already protect the patient's personal data and which are tailored to the context of medical care. Accordingly, in the Dutch Act implementing the GDPR, for example, it is explicitly acknowledged that the national patient confidentiality law continues to exist and, as a *lex specialis*, prevails over the GDPR. Given the diverging interests and the liabilities at stake, the issue of whether the GDPR applies to the provision of medical care is likely to end up before the Court of Justice of the EU, where it might suffer the same fate as the EU Data Retention Directive [8].

A case against Myriad or against the doctor?

A second preliminary issue facing patients invoking the GDPR to gain access to all their genetic data is whom to turn to? The GDPR grants data subjects a number of rights (data subject rights) vis-a-vis the controller of the personal data, who has the corresponding obligation to respond to requests for and facilitate the exercise of these rights, barring any exceptions. That raises the question of who controls the genetic data produced in a clinical setting by a genetic testing company? The GDPR defines a controller as 'the natural or legal person, (..) which, alone or jointly with others, determines the purposes and means of the processing of personal data'. The work and data flow in a typical setting for clinical genetic testing has been illustrated in Fig. 1. In such a setting, it is the clinician and not the testing company, who decides whether or not to order a genetic test and so determines the purposes and the means of the processing of the genetic data. A third party laboratory may only process confidential patient data if and to the extent instructed by the clinician. Accordingly, Myriad makes it plain to its customers that 'while genetic testing and medical society guidelines provide important and useful information, all medical management decisions should be made based on consultation between each patient and his or her healthcare professional' [9]. Consequently, the testing company would qualify as the processor of this data, acting on behalf of, and at the instruction of, the clinician as the controller. Whether this qualification may change over time, as testing companies may come to be seen as 'co-providers of clinical care' and hence as 'joint controllers', is an open question.

The GDPR requires that when a controller (in casu: the clinician) outsources a certain processing (in casu genetic testing) to a third party (in casu: the testing company), such outsourcing must be governed by a contract between the controller and the processor. This contract must stipulate that the processor assists the controller, by appropriate technical and organizational measures, insofar as this is possible, to satisfy his obligation to respond to requests from data subjects for exercising their rights. Hence, a clinician ordering a genetic test from Myriad must stipulate

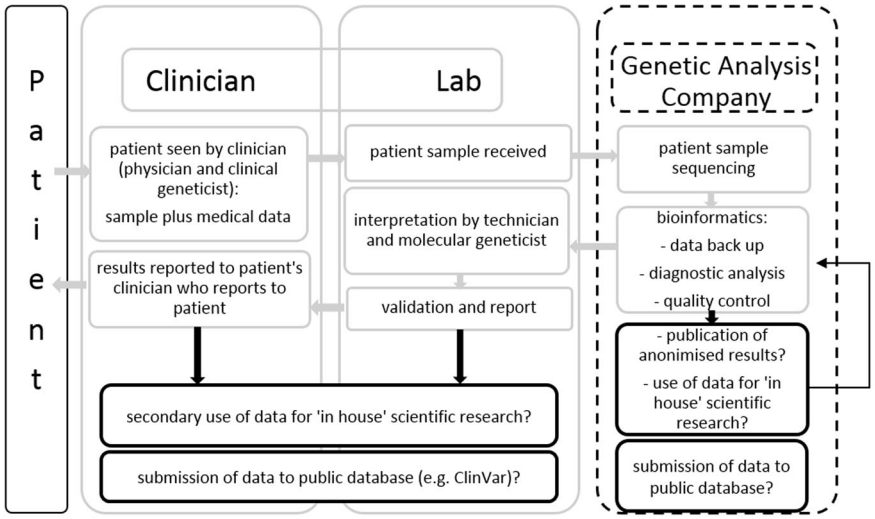

Fig. 1 Work and data flow during genetic testing

Legend – Gray colour arrows and boxes represent clinical genetics work and data flow; black ---- colour boxes represents activities of genetic testing company; black colour arrows and boxes represent publication and possible secondary use of data for scientific research purposes.

in the agreement that the latter is to assist the clinician in meeting such requests . Under the GDPR, a patient should direct her requests for access in principle to his/her clinician, who should then call, on behalf of the patient and on the basis of the agreement with Myriad, on Myriad for assistance in meeting the request. That leads to the next question, i.e., what is the scope of the GDPR rights?

The scope of the access right

The GDPR access right comprises the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to and a copy of the personal data and certain information relating to the data. The right applies to all personal data 'undergoing processing'. Applied to the context of genetic testing, that seems to include not only the Myriad test results, but also the information beyond the test report, such as the raw genomic sequencing reads, assembled sequences of the genes examined, and variants Myriad classifies as clinically insignificant [10]. Under the GDPR, Myriad must provide modalities to facilitate the exercise of this access right, and where possible, provide remote access to a secure system providing the data subject with direct access to her personal information. For a number of reasons, however, providing all these types of information to individual patients may be problematic. First, medical management decisions made on the basis of variant interpretations are crucial to the safety and well-being of patients. Myriad itself has pointed out that variant classification databases used for clinical purposes should be subjected to regulatory oversight, as the use of unregulated databases poses risks to patients. Therefore, the information must be subjected to confirmatory analysis. Second, the information may amount to false positives or false negatives, or lack analytical validity or clinical utility. Thus, providing unconditional access to that kind of information may violate professional standards of care. Compounding matters are the European ethical standards mandating that genetic test results may not be provided to patients without proper genetic counselling [11, 12]. This opens up the additional question of whether the GDPR access right could trump statutory and professional limitations on providing certain types of data to patients? Applied to clinical genetic testing, must sequence data which, for medical–professional reasons, are not part of the medical record and not clinically actionable, nevertheless be provided to patients on the basis of the GDPR access right? Even if providing this 'information' could expose the provider to civil or even criminal liability? US citizens may be keen to claim access, but they are also keen to claim damages, especially in the area of healthcare. The fact that the GDPR access right as applied in the context of clinical information leaves no room for the above clinical considerations and statutory limitations illustrates the point made earlier that the GDPR is not fit for application to medical records in the first place.

The right to the algorithm

A related issue is that Myriad's algorithms are critical to understanding the clinical significance of genetic variants. This raises the question of whether these algorithms are individually identifiable to the patients and hence constitute

personal data. While pure algorithms do not identify individuals, data related to the applications of these algorithms to specific individuals could qualify as such when they include personal data [13]. Whether that means that this data become subject to the access right is an open question. Even if it does, however, it should not adversely affect the copyright protecting the software [14].

The right to data portability

One of the two motivations of the US patients to claim access to their full genetic information held by Myriad was to share these data with the scientific research community. The GDPR provides for a novel right that seeks to bestow that kind of control over one's personal data: the right to 'data portability'. This right comprises both the right to receive, in a structured, commonly used and machine-readable format, the personal data which a data subject has provided to the controller, and the right to have these data transmitted directly to a third party. In the case of clinical genetic testing, that could include the research community, but also competing testing companies. The right to data portability applies where the processing of personal data is based on consent or on a contract, and the processing is carried out by automated means. It is expressly limited, however, to the personal data which the data subject has provided to the controller. This includes both data actively and knowingly provided by the data subject (e.g., mailing address, user name) and data observed by the controller by virtue of the use of the service or device by the data subject (e.g., a person's search history, location data or a heartbeat tracked by a fitness tracker) [15]. The right would not extend to data 'inferred' or 'derived' by the controller from the data provided by the data subject, e.g. a profile created in the context of risk management. As the genomic data produced by Myriad, such as the raw genomic reads and even the genetic test results, are not provided by the data subject but inferred by Myriad from the data (sample) provided by the patient, these data are not subject to the right to data portability.

Access right versus database right

In addition to access and portability rights, the GDPR introduces mechanisms enabling class actions for data subjects. In theory then, a class action of multiple patients invoking their access right would enable them to reconstruct, base by base, Myriad's databases and make them available for the research community or other parties. Such a move would challenge Myriad's business model which, after its genetic testing patents have been partially invalidated, is now allegedly based on its proprietary databases. To ward off such a class action, Myriad could claim that its databases are eligible for legal protection under the EU Database Right. This right grants database builders the right to prevent extraction or reutilization of substantial parts of their database [16]. The database right is not absolute however. Its holder may not prevent a lawful user of the database from extracting and/or reutilizing parts of its contents that are insubstantial, evaluated qualitatively or quantitatively, 'for any purpose whatsoever'. Patients could argue that they qualify as a 'lawful user' of Myriad's databases and that their individual requests for access to their individual personal information contained in these databases only covers an insubstantial part thereof. However, the right to extract or reutilize an insubstantial part of the database only applies to databases which have been made available to the public, in 'whatever manner'. The precise meaning of this prerequisite is not entirely clear but, to our knowledge, Myriad does not routinely make its databases publicly available [17]. Another argument would be that the right to claim an insubstantial part may not conflict with the 'normal exploitation of the database or unreasonably prejudice the legitimate interests of the maker of the database'. Alternatively, patients could claim that the database right only pertains to the collection of data as such, leaving third party individual rights to the constituent data intact. The database right does not preclude, for example, anyone from exercising his/her individual data protection access right with respect to personal data contained in the database [18]. This avenue too, however, cannot give ground to circumvent Myriad's database rights. First, the access right under the GDPR is not an absolute right, just as the general right to protection of personal data is not an absolute right. It must be considered in relation to its function in society, it must be balanced against other rights and freedoms, and may not adversely affect trade secrets or intellectual property, including database rights. Second, the database right does not allow repeated and systematic extraction and/or reutilization of insubstantial parts which conflict with a normal exploitation of the database.

Is research none of Myriad's business?

The first question then is what, exactly, amounts to a 'normal exploitation' of a genetic database generated by a genetic testing company? Is 'normal exploitation' limited to selling the test results, or does it include, if not require, the conduct of scientific research on the data the company has generated? According to the US complainants and their academic supporters, the only way to advance research would be for the data to be available to the academic research community in public databases [4]. Myriad might want to claim that doing research is part of its normal business, by pointing out that its products require continuous investments in fundamental research . Notably, the GDPR defines scientific research as including not only fundamental research but also

applied research and privately funded research. The second question is whether the exercise of the GDPR access right would conflict with this normal exploitation? It is obvious that patients are free to share their test results with the public. However, using the access right to claim data beyond the tests results in order to make these data also public, is equally obvious to conflict with Myriad's normal exploitation of these data, as it would be hard to prevent Myriad's competitorsfrom having a free ride.

Conclusions

Pursuant to EU law, the GDPR does not apply to the practice of medicine and hence the medical record. For data outside the medical record, exercise of the GDPR access right may be limited to the extent that its exercise would result in the violation of medical-professional norms, expose the testing company to potential liability, or compromise normal exploitation of the database of which the personal data form part.

Acknowledgements This article is based on the Legal Expert Report prepared by Jasper Bovenberg in 2016 as part of the EU funded Project: the Genetics Clinic of the Future (GCOF) for the lead beneficiary: Institute of Technology of Biology and Chemistry (ITQB), Portugal, Mara Almeida.

Funding The Genetics Clinic of the Future (GCOF) is a Coordination and Support Action funded by the European Union under the section Health, Demographic Change and Wellbeing of the Horizon 2020 Programme, Grant Agreement no. 643439. Mara Almeida would also like to acknowledge the support from theFundação para Ciência e a Tecnologia (FCT) of Portugal (CFCUL/FIL/UID0678).

Compliance with ethical standards

Conflict of interest The authors declare that they have no conflict of interest.

References

1. US Supreme Court. Association for Molecular Pathology v. Myriad Genetics, 133 S. Ct. 2107, 2013.
2. Health Information Privacy Complaint against Myriad, 19 May 2016. https://Www.Aclu.Org/Legal-Document/Aclu-Hipaa-Complaint.
3. Kevin Davies & Michael White, quoted in Health Information Privacy Complaint; Turna Ray, GenomeWeb, 5 April 2016.
4. HHS, Individuals' rights under HIPAA to access their health information, 7 January 2016. https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/index.html#maximumflatfee.
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).
6. Articles 7 and 8 of the Charter of Fundamental Rights of the European Union, 26 October 2012.
7. The Treaty on EU. E.g., Court of Justice of the EU, Philipp Morris, C-547/14, EU: C: 2016: 325, 4 May 2016.
8. CJEU, Joined Cases C-293/12, and C-594/12.
9. Myriad Genetic Laboratories. https://myriad.com/healthcare-professionals/improving-patient-care/predicting-disease/.
10. Myriad letter to patient, Exhibit 2 to the Complaint, 11 March 2016.
11. Article 5 Additional Protocol to the Convention on Human Rights and Biomedicine, concerning Genetic Testing for Health Purposes, Strasbourg, 27 November 2008.
12. Thorogood A, Bobe J, Prainsack B, Middleton A, Scott E, Nelson S, et al. APPLaUD: access for patients and participants to individual level uninterpreted genomic data. Hum Genom. 2018;12:7.
13. Guerrini CJ, McGuire AL, Majunder MA. Myriad take two: can genomic databases remain secret? Science. 2017;356:586–7.
14. Recital 63 of the GDPR.
15. EU, Article 29 Data Protection Working Party, 16/EN WP 242 rev. 01, Guidelines on the right to data portability, 5 April 2017.
16. Bovenberg JA. Should companies set up databases in Europe? Nat Biotechnol. 2000;18:907.
17. Cook-Deegan R, Conley JM, Evans JP, Vorhaus D. The next controversy in genetic testing: clinical data as trade secrets? Eur J Hum Genet. 2013;21:585–8.
18. Article 13 of the Directive 96191 of the European Parliament and of the Council on the Legal Protection of Databases, 11 March 1996.