(2018) 26 JLM 23

THE EUROPEAN UNION GENERAL DATA PROTECTION REGULATION (EU 2016/679) AND THE AUSTRALIAN MY HEALTH RECORD SCHEME – A COMPARATIVE STUDY OF CONSENT TO DATA PROCESSING PROVISIONS

Danuta Mendelson,

Chair in Law (Research), School of Law, Deakin University. This study incorporates a paper on the EU General Data Protection Regulation and the My Health Record scheme presented at the 20th Congress of the International Academy of Comparative Law, Fukuoka 22–28 July 2018.
Correspondence to: danuta.mendelson@deakin.edu.au

Citation: Danuta Mendelson, "The European Union General Data Protection Regulation (Eu 2016/679) and the Australian My Health Record Scheme – A Comparative Study of Consent to Data Processing Provisions" (2018) 26 *Journal of Law and Medicine* 23-38

ABSTRACT

As a general rule, lawfulness of data processing under the European Union General Data Protection Regulation (EU 2016/679) (GDPR) is based on affirmative, unambiguous, voluntary, informed, and specific or "granular" consent to processing of their data, including health data, by individuals referred to as data subjects. The GDPR grants data subjects the legal right to specifically agree to (or refuse) having their data processed in any of the ways statutorily defined as "processing". Individuals also have the legal right to be fully informed about each and every intended use of their data by data processors and controllers, and the right to refuse such use. In Australia, once registered on the My Health Record (MHR) system, "healthcare recipients" as patients-cum-data subjects are called under the MHR scheme, have the right to remove documents from their MHR files and block some health care providers from accessing their data. However, this study demonstrates that the notion of "standing" consent that the MHR scheme appears to have created does not conform to any of the principles and rules governing data subjects' consent rights under GDPR.

Keywords - electronic health records - EU General Data Protection Regulation - consent - My Health Record scheme - patients - data subjects

> "If it is correctly used, consent is a tool giving the data subject control over the processing of his data. If incorrectly used, the data subject's control becomes illusory and consent constitutes an inappropriate basis for processing."[1]

I. Introduction

[1] Opinion 06/2014 on the Notion of Legitimate Interests of the Data Controller under Article 7 of Directive 95/46/EC, WP217 (adopted 9 April 2014) 16 (Opinion). The Opinion was adopted and expanded in Guidelines on Consent under Regulation 2016/679, WP259 (revised and adopted 10 April 2018) 3.

On 25 May 2018 the General Data Protection Regulation (EU 2016/679) (GDPR)[2] came into operation, replacing the Data Protection Directive 95/46/EC.[3] Unlike the Directive, which in order to be legally binding had to be enabled by each European Union member state enacting its own data protection legislation, the Regulation is directly binding and applicable on all 27 European Union member states.[4]

While analysis relating to the GDPR has largely focused on how its privacy and security protections impact on Australian businesses,[5] this European Union law also should be discussed in reference to the requirement of consent as an element of its protection of natural persons' fundamental rights "in relation to the processing of personal data."[6]

The GDPR is primarily concerned with delineating requirements for lawful processing of personal data, with the term "processing" non-exhaustively defined in Art 4(2) as:

> any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.[7]

Article 8 of the European Union Charter of Fundamental Rights[8] stipulates that for data processing to be legitimate (lawful), personal data must be processed "on the basis of the consent of the person concerned or some other legitimate basis laid down by law".[9] For the purposes of GDPR, as a general rule, "consent can only be an appropriate lawful basis [for data processing] if a data subject is offered control and is offered a genuine choice with regard to accepting or declining the terms offered or declining them without detriment".[10] Therefore, in terms of fundamental rights, when "control [is] exercised through consent … an individual's decision to accept a data processing operation should be subject to rigorous requirements, particularly taking into account that in doing so, an individual may be waiving a fundamental right".[11] According to GDPR Recital 32, consent:

---

[2] General Data Protection Regulation (EU) No 2016/679 of the European Parliament and of the Council on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data (GDPR) [2016] OJ L 119/1.

[3] GDPR, n 2, Art 94, repeals Directive 95/46/EC.

[4] GDPR, n 2, Recitals 10, 12.

[5] See, eg, Office of the Australian Privacy Commissioner, Privacy Business Resource 21: Australian Businesses and the EU General Data Protection Regulation (updated June 2018)

[6] GDPR, n 2, Recital 1. The term "data-subjects" is used to describe natural persons whose personal data is processed by a controller or processor.

[7] GDPR, n 2, Art 4(2).

[8] European Union Charter of Fundamental Rights (ratified 7 December 2000) Art 8. By virtue of the Treaty of Lisbon and Treaty on the Functioning of the European Union opened for signature 7 February 1992, [2012] OJ C 326/47 (entered into force 1 November 1993). Under Art 6(1), European Union Charter of Fundamental Rights has "the same legal value as the Treaties".

[9] European Union Charter of Fundamental Rights, Art 8(2).

[10] Guidelines on Consent under Regulation 2016/679, n 1, 3.

[11] Opinion 15/2011 of the Article 29 Data Protection Working Party on the Definition of Consent, WP187 (adopted 13 July 2011) 8. The notion of consent as fundamental right is supported in the Guidelines on Consent under Regulation 2016/679, n 1, 3.

> "should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement. … Silence, pre-ticked boxes or inactivity should not therefore constitute consent. Consent should cover all processing activities carried out for the same purpose or purposes".[12]

The "crucial role of consent"[13] in determining the lawfulness of personal data processing under GDPR is relevant to the Australian My Health Record (MHR) scheme,[14] partly because it can serve as a model for comprehensive implementation of the principle that data subjects have a right to control over the use that is being made of their data (see below), and partly because of its extra-territorial reach.

This comparative study does not discuss security and privacy aspects of National Electronic Health Records (NEHR) systems run by public authorities; rather, the analysis concentrates consent as a critical element in protecting individual patients' rights with respect to the processing of their personal health data under GDPR and under the Australian MHR legislative scheme. Australia does not have

the European Commission's certificate of adequate level of data protection.[15] One of the reasons might be the less than impressive approach to consent in its framework of protections for patients' rights in relation to health and clinical data processing.

This analysis is divided into five parts. The second part surveys the relevant principles and rules of the GDPR including its extra-territorial reach. The third part provides an example of how the interface between the European Union and Australian data-processing frameworks might arise; the fourth examines the applicability of GDPR to NEHRs schemes, and the major elements required for valid consent under GDPR. The fifth part discusses the MHR legal framework in relation to patients' consent, contrasting it with the protections afforded under GDPR. The study adopts the GDPR terminology as more accurate and widely accepted than terms and phrases coined in the MHR legislation, except when referring to the Australian statutes, Rules, Regulations and Guidelines.

II. Extra-territorial Reach of the GDPR

[12] GDPR, n 2, Art 4(11) defines consent as "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her".

[13] Guidelines on Consent under Regulation 2016/679, n 1, 3.

[14] For a detailed discussion of the My Health Records scheme see, D Mendelson and G Wolf, ""My [Electronic] Health Record" – Cui Bono (for Whose Benefit)?" (2016) 24 JLM 283; D Mendelson and G Wolf, "Privacy and Confidentiality" in I Freckelton and K Petersen (eds), Tensions and Traumas in Health Law (Federation Press, 2017) Ch 14, 266–282.

[15] GDPR, n 2, Art 45 empowers the European Commission to determine whether a country outside the European Union offers an adequate level of data protection, whether by its domestic legislation or of the international commitments it has entered into.

Recital 17 and Art 2(3) of the GDPR, specify that its "material scope"[16] encompasses Regulation (EC) No 45/2001[17] and other European Union legislation that govern "the processing of personal data by the Union institutions, bodies, offices and agencies" mandating that these instruments "shall be adapted to the principles and rules of this Regulation". Therefore, in the European Union, public administration entities established for purposes of processing personal health data of natural persons, for example patients, would be subject of the GDPR rules (including derogations).[18] The MHR scheme fits the definition of a public administration entity in the third country.[19] Additionally, some of its other functions suggest that arrangements for processing of patients' personal data can be considered as business transactions. In particular, the Practice Incentives Program eHealth Incentive[20] enables participating general practitioners[21] and nurse practitioners[22] to upload on the MHR system "over the quarter, 5 shared health summaries for one patient or 1 shared health summary for each of 5 patients or any combination amounting to 5"[23] for "a maximum payment of $A12,500 per quarter".[24] Although the incentive payments

[16] For limitations on applicability of the GDPR, n 2, see Art 2(2).
[17] The European Data Protection Supervisor is an independent supervisory authority that scrutinises whether European institutions and bodies fulfilling their obligations to respect natural persons' right to privacy and data protection when their personal data is processed.
[18] GDPR, n 2, Art 49 on derogations (exemptions from or relaxation of GDPR rules) in the context of transfers of personal data to third countries.
[19] GDPR, n 2, Art 44.
[20] Australian Government, Australian Digital Health Agency, Practice Incentives Program (PIP) eHealth Incentive <https://www.myhealthrecord.gov.au/for-healthcare-professionals/practice-incentives-program>; Australian Government, Department of Human Services, Practice Incentives Program <https://www.humanservices.gov.au/health-professionals/services/medicare/practice-incentives-program>.
[21] "General Practitioners (GPs) include GPs or non-specialist medical practitioners, known as other medical practitioners, who provide non-referred services but are not GPs. GPs include: Fellows of the Royal Australian College of General Practitioners (RACGP) and the Australian College of Rural and Remote Medicine; vocationally registered general practitioners, and medical practitioners undertaking approved training". Australian Government, Department of Human Services, Practice Nurse Incentive Program <https://www.humanservices.gov.au/organisations/health-professionals/services/medicare/practice-incentives-program>.
[22] Australian Government, Department of Human Services, n 21.
[23] See Australian Government, Australian Digital Health Agency, n 20. Participating practices are required to upload Shared Health Summaries for a minimum of 0.5% of the practice's standardised whole patient equivalent (SWPE); the latter is defined as "value of a practice [that] is the sum of the fractions of care provided to practice patients. This is weighted for the age and gender of each patient". Australian Government, Department of Human Services, n 21.
[24] Australian Government, Department of Human Services, Practice Incentives Program eHealth Incentive Guidelines (May 2016); see also, Lynne Minion, RACGP Claims Gaining Patient Consent for My Health Record Uploads Is Not the Job of Doctors and Calls for Improved Incentives, Healthcare IT (6 July 2018) <https://www.healthcareit.com.au/article/racgp-claims-gaining-patient-consent-my-health-record-uploads-not-job-doctors-and-calls>.

can be interpreted as recompense for ensuring compliance with the software system requirements and for the effort of uploading shared health summaries, in essence, they are commercial transactions whereby general practitioners and nurse practitioners sell, for an agreed sum, personal information obtained from patients by uploading it on the MHR system.[25]
In terms of "territorial scope", according to Recital 14 of the GDPR, its protections "should apply to natural persons, whatever their nationality or place of residence, in relation to the processing of their personal data".

Article 3 provides that GDPR applies processing of personal data by a "controller", or "processor" "regardless of whether the processing takes place in the Union or not".[26] For the purposes of GDPR, "controller" is defined as any "natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data".[27] This definition, as will be discussed below, fits in with the functions of the Australian Digital Health Agency, which is the System Operator of the Australian NEHRs system known as the MHR scheme.[28]

The term, "processor" refers to "a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller".[29] Thus, any healthcare professional who creates, retrieves, uses or disseminates via an electronic system a record that includes patient's personal data (name, age, gender, Medicare number, e-mail address, etc), would qualify as a processor.

The GDPR also applies to “the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:

> (a) the offering of … services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union;
> (b) the monitoring of their behaviour as far as their behaviour takes place within the Union”.[30]

III. Interface between GDPR and MHR Scheme

---

[25] As of 1 July 2018, there were 6,483 General Practice Organisations; presumably, most of them would be involved in Australian Government, Australian Digital Health Agency, n 20 <https://www.myhealthrecord.gov.au/sites/g/files/net4206/f/my_health_record_dashboard_-_1_july_2018.pdf?v=1530681843>.
[26] GDPR, n 2, Recital 22, "The legal form of such arrangements, whether through a branch or a subsidiary with a legal personality, is not the determining factor in that respect"; Australian Government, Department of Human Services, n 21
[27] GDPR, n 2, Art 4(7).
[28] *My Health Records Act 2012* (Cth) s 14; My Health Records Regulation 2012 (Cth) reg 2.1.1.
[29] GDPR, n 2, Art 4(8).
[30] GDPR, n 2, Art 3(3) provides additionally that it "applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law".

With its wide extra-territorial applicability, GDPR's rules and principles are germane to all EHRs' systems, irrespective of their geographical location.[31] The following example illustrates the relevance of GDPR to MHR scheme.
Health care data generated by people in countries outside the European Union (eg, Australians in Australia, Japanese in Japan, etc) are governed solely by the law of that country (Australia, Japan, etc), not the GDPR. However, since the GDPR applies to all patients who are located in any European Union country, whatever their nationality or place of residence, any health care data created in the European Union for them will have to comply with the GDPR rules.[32] This is equally applicable to tourists, residents and persons with dual citizenship, for example, Australians with Australian and European Union citizenship.

The following scenario can serve as an illustration of how the GDPR works vis-a-vis non-European Union countries. A European Union doctor, having seen Ms Drocer,[33] an Australian staying in Paris,

sends the electronic report (data) to the patient's general practitioner in Melbourne, who then uploads it on the MHR system. The European Union doctor when handling Ms Drocer's data must adhere to the GDPR, but at this stage, theoretically, neither the Australian general practitioner as the processor, nor the MHR system as the controller of Ms Drocer's information need to refer to the GDPR rules and requirements. After her return to Australia, in accordance with recommendations and information provided by the European Union doctor that her general practitioner uploaded on the MHR system, Ms Drocer undergoes follow-up treatment. She then goes back to Paris (or any other place in the European Union), and a European Union doctor requests her follow-up data from the practitioner. Once such request, originating in the European Union is made, both the general practitioner and the MHR system will become subject to the GDPR in respect of the data that was generated in the European Union by the French doctor.[34]

What are Ms Drocer's rights of consent, refusal and withdrawal of consent regarding data processing of her personal, including health, information under GDPR and MHR legislation? Irrespective of whether the GDPR's imposition of extra-territorial jurisdiction on non-European Union countries might be open to challenge, it is pertinent to compare the relevant provisions of GDPR with Australian legislative framework that governs its NEHRs system in relation to the individuals' right to data protection. In particular, it is apposite to discuss a sharp divergence that exists between, among other matters, the approach to consent in the context of data subjects' rights as codified in the GDPR and in Australian MHR legislation.

---

[31] GDPR, n 2, Recital 2: "The principles of, and rules on the protection of natural persons with regard to the processing of their personal data should, whatever their nationality or residence, respect their fundamental rights and freedoms, in particular their right to the protection of personal data."
[32] RZ Arndt, "Privacy Gets Complicated for Data Crossing the Pond", Modern Healthcare, 21 May 2018, 0004.
[33] Ms Drocer made her first appearance in D Mendelson, "Travels of a Medical Record and the Myth of Privacy" (2003) 11 JLM 136, which examined the erosion of patients' right to medical confidentiality in the administrative state.
[34] This example is an adaption of one provided by Arndt, n 32, 0004.

The discussion will focus on the rights of consent, refusal and withdrawal of consent by competent adults,[35] and proceed from general overview of the GDPR and the regulatory framework governing MHR scheme to more granular comparison of their respective privacy principles and requirements.

GDPR and NEHRs Systems

European Union jurisprudence distinguishes between the general right of privacy on the one hand and a right to data protection on the other, "as two distinguishable, but connected rights".[36] Privacy is protected under Art 7 of the EU Charter of Fundamental Rights, and data protection, which is the focus of this analysis, falls under Art 8.[37] It states that "natural persons should have control of their own personal data", and "consent is recognised as an essential aspect of the fundamental right to the protection of personal data" (although it is not the only legal ground enabling lawful processing of personal data).[38]

Article 4(1) of the GDPR defines "personal information" as:

> "any information relating to an identified or identifiable natural person ("data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person".[39]

In the context of GDPR, data contained in any EHR are, by definition, "data concerning health", namely, "personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status".[40]

---

[35] Rights of minors and incompetent adults under GDPR and My Health Record system deserve a thorough examination that is beyond the scope of this analysis. Likewise, study does include consent of data subjects in relation to the use of their data for research, law enforcement and national security purposes.

[36] J Reichel, "Oversight of EU Medical Data Transfers – An Administrative Law Perspective on Cross-border Biomedical Research Administration" (2017) 7 Health Technol 389, 389, citing S Slokenberga, European Legal Perspectives on Direct-to-Consumer Genetic Testing (June, 2016) Ch 4.

[37] EU Charter of Fundamental Rights, Art 8: "1. Everyone has the right to the protection of personal data concerning him or her. 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. 3. Compliance with these rules shall be subject to control by an independent authority" <http://fra.europa.eu/en/charterpedia/article/8-protection-personal-data>.

[38] GDPR, n 2, Recital 7.

[39] GDPR, n 2, Recital 4 further states that: "The processing of personal data should be designed to serve mankind. The right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality."

[40] GDPR, n 2, Art 4(15).

IV. Applicability of GDPR to NEHRs Systems and the Requirement of Patients' Valid Consent

NEHR systems operate under the responsibility of the relevant national health authority, and their functions include storing and managing these records with an aim typically to "make a patient's medical history available to health professionals in health care institutions and provide linkages to related services such as pharmacies, laboratories, specialists, and emergency and medical imaging facilities".[41] All functions of the authority operating NEHR system come within the scope of "processing". This means that each of the enumerated operations under Art 4(2) of the GDPR has to comply with GDPR privacy requirements and can be subject to the scrutiny of such compliance by state supervisory authorities of the individual European Union Member.[42]

As noted above, the principle that consent is an essential aspect of the fundamental right to the protection of personal data[43] underpins EHRs systems created by the European Union member states, even though, by virtue of Art 168(7) of the Lisbon Treaty, they retain the power to manage their own health services.[44] European Commission adopted its initial eHealth Action Plan[45] in 2004 to foster electronic "interaction between patients and health-service providers, institution-to-institution transmission of data, or peer-to-peer communication between patients and/or health professionals".[46] The majority of the 27 member states either have implemented, or are developing, shared EHRs models,[47] though

---

[41] World Health Organisation [WHO], Report of the Third Global Survey on eHealth 2016, 94 <http://apps.who.int.ezproxy-b.deakin.edu.au/iris/bitstream/10665/252529/1/9789241511780-eng.pdf#page=118>.

[42] GDPR, n 2, Art 51(1) provides that "Each Member State shall provide for one or more independent public authorities to be responsible for monitoring the application of this Regulation, in order to protect the fundamental rights and freedoms of natural persons in relation to processing … of personal data". See also Art 83(1).

[43] Opinion 15/2011 of the Article 29 Data Protection Working Party on the Definition of Consent, n 11, 5; Guidelines on Consent under Regulation 2016/679, n 1, 3.

[44] Under Treaty on the Functioning of the European Union, Art 168(2) and (7), while the European Union has a duty to "encourage cooperation between the Member States … to improve the complementarity of their health services in cross-border areas", the member states have the responsibility for defining "their health policy and for the organisation and delivery of health services and medical care", including "the management of health services and medical care and the allocation of the resources assigned to them". Source: Treaty on the Functioning of the European Union, opened for signature 7 February 1992, [2012] OJ C 326/47 (entered into force 1 November 1993), Title XIV *Public Health Act* 168.

[45] Commission of the European Communities, e-Health – Making Healthcare Better for European Citizens: An Action Plan for a European e-Health Area (2004) <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2004:0356:FIN:EN:PDF>.

[46] European Commission, eHealth Action Plan 2012–2020: Innovative Healthcare for the 21st Century (7 December 2012) [1] <https://ec.europa.eu/health/sites/health/files/ehealth/docs/com_2012_736_en.pdf>.

[47] EU Health Programme (2008–2013), "Overview of the National Laws on Electronic Health Records in the EU Member States and Their Interaction with the Provision of Cross-border eHealth Services", Final Report and Recommendations (July 2014); "EHRs are in use in all countries covered by this Study and there are numerous forms of EHRs at all levels of the healthcare sector of most countries." See also European Commission, n 46.

only few have nationally centralised systems,[48] and as of 2 June 2017, even fewer have reported "specific legislation governing the use of the national electronic health records [NEHR] system".[49]

All NEHR-related legislation enacted by European Union Member countries must comply with legal instruments such as the EU Charter of Fundamental Rights; Regulation (EC) No 45/2001 of the European Parliament and of the Council,[50] the Patients' Rights Directive 2011/24/EU and others,[51] that aim to achieve "a high level of trust and security" for patients' data in the of electronic health summaries.[52] There are also guidelines,[53] including the 2016 European eHealth Network's[54] Guideline on Electronic Exchange of Health Data,[55] a non-

[48] As of 2 June 2017, an NEHR system, as defined in the 2015 WHO Global eHealth Survey, existed in 29 countries of the European region: Albania, Austria, Azerbaijan, Belgium, Bosnia and Herzegovina, Cyprus, Denmark, Estonia, Finland, Iceland, Israel, Italy, Kazakhstan, Kirgizstan, Lithuania, Luxemburg, Montenegro, Norway, Portugal, Montenegro, Republic of Moldova, Romania, Russian Federation, San Marino, Spain, Tajikistan, Turkey, Turkmenistan, Uzbekistan (France and Germany did not participate in the Survey). European Health Information Gateway, National EHR System Exists <https://gateway-euro-who-int.ezproxy-b.deakin.edu.au/en/indicators/ehealth_survey_84-has-a-national-ehr-system/visualizations/#id=31759&tab=table>.

[49] Albania, Austria, Azerbaijan, Belgium, Bosnia and Herzegovina, Cyprus, Estonia, Finland, Iceland, Italy, Lithuania, Luxemburg, Montenegro, Norway, Portugal, Spain, Turkey, Turkmenistan reported that they had "specific legislation governing the use of the NEHR system" as of 2 June 2017; European Health Information Gateway, Specific Legislation Governing the Use of the National Electronic Health Record (EHR) System Exists <https://gateway-euro-who-int.ezproxy-b.deakin.edu.au/en/indicators/ehealth_survey_14-legislation-on-use-of-national-ehr-system/visualizations/#id=31693&tab=table>.

[50] Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the Protection of Individuals with Regard to the Processing of Personal Data by the European Community Institutions, Bodies, Offices and Agencies [2001] OJ L 8/1, 12.1.2001. This Regulation is in the process of being adapted to reflect GDPR.

[51] The European Convention on the Protection of Human Rights and Fundamental Freedoms (1950), the Social Charter (1961, revised and expanded in 1996); the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data Council of Europe (1980).

[52] The eHealth Network, Guideline on Electronic Exchange of Health Data, [1.3] <https://ec.europa.eu/health/sites/health/files/ehealth/docs/ev_20160607_co05_03_en.pdf>.

[53] UN Guidelines Concerning Computerized Data Files (1990); OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (2013), C(80)58/final, as amended on 11 July 2013 by C (2013)79.

[54] The eHealth Network is a voluntary network, set up under Directive 2011/24/EU, Art 14, which provides a platform of member states' competent authorities dealing with eHealth, n 52. The eHealth Network Guideline on Electronic Exchange of Health Data under the Cross-border Directive 2011/24/EU, Art 2 defines "interoperability" within the context of European public service delivery as "the ability of disparate and diverse organisations to interact towards mutually beneficial and agreed common goals, involving the sharing of information and knowledge between the organisations, through the business processes they support, by means of the exchange of data between their respective ICT systems (European Interoperability Framework)".

legally binding "reference" on standards for legal, organisational, semantic and technical interoperability[56] to support e-health care across borders of European Union member states, as well as at national level.[57] However, GDPR is the most important instrument because of its directly binding nature.

NEHR schemes fall prima facie within the ambit of Art 9(1) of the GDPR, which prohibits processing of "special category of personal data", including "data revealing racial or ethnic origin, … data concerning health or data concerning a natural person's sex life or sexual orientation".[58] However the exception (derogation) to Art 9(1) listed in Art 9(2)(g) of the GDPR removes the prohibition where "processing is necessary for reasons of substantial public interest", and all NEHR systems would claim as their raison d'etre substantial public benefits.[59] Under this derogation, the processing of data concerning health must be:

> "proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject".[60]

Elements of Valid Consent

The Art 9(2)(g) of the GDPR derogation imposes three data protection obligations: (1) application of proportionality principle, (2) respect for the "essence of the right to data protection" (presumably includes the control by patients over "their own personal data")[61] and (3) consent. In relation to consent, Art 6(1) of the GDPR provides that:

> "processing shall be lawful only if and to the extent that at least one of the following applies: the data subject has given consent to the processing of his or her personal data for one or more specific purposes".[62] [62]

---

[55] The eHealth Network, n 52.

[56] The eHealth Network, n 52.

[57] The eHealth Network, n 52, Art 1.

[58] GDPR, n 2, Art 9(1) Processing of special categories of personal data.

[59] EHRs also could possibly fall under derogation in GDPR, n 2, Art 9(2)(h): "processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3". However, since all of the purposes are achievable without the national EHRs, the latter cannot be validly characterised as "necessary".

[60] GDPR, n 2, Art 9(2)(g).

[61] GDPR, n 2, Recital 7.

[62] Five other grounds for lawful processing listed in GDPR, n 2, Art 6(1) include legal obligations under contracts, and "the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller"; the necessity to protect "the vital interests of the data subject or of another natural person"; and necessity based on "the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data … Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks."

However, in relation to public authorities, Recital 43 of the GDPR imposes a presumption that the imbalances of power between public authorities as controllers and individual data subjects make it unlikely that the latter's "consent was freely given in all the circumstances of that specific situation". Therefore, consent will not provide "a valid legal ground for the processing of personal data" unless the public authority can demonstrate that a separate consent was given "to different personal data processing operations"[63] (if it is "appropriate in the individual case"). It is one of the conditions for valid consent under Art 7 of the GDPR that in cases of processing based on consent, "the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data". These rules are of particular importance to NEHR systems, which involve multiple processing operations.

Therefore, in the European Union before uploading Ms Drocer's personal data on an NEHR system, the European Union NEHR scheme, or rather the European Union doctor acting on its behalf, would be required to obtain from the patient a valid consent that comprises of four elements stipulated in Art 4(11) of the GDPR, namely: "freely given, specific, informed and unambiguous indication" of her wishes "by a statement or by a clear affirmative action", that "signifies agreement to the processing of personal data relating to him or her".

To give her consent freely, Ms Drocer must be given a real choice and must not feel compelled to consent.[64] Her free consent must be also "granular". For example, if the particular NEHR uses uploaded personal data for purposes that are not of immediate therapeutic benefit to the patient (eg research, tracing drug/medication use, health insurance, etc.),[65] the European Union doctor must inform the patient of each specific purpose and obtain a separate additional consent for these other purposes.[66]

Indeed, under Recital 43 of the GDPR "consent is presumed not to be freely given if the process/procedure for obtaining consent does not allow data subjects to give separate consent for personal data processing operations respectively … despite it being appropriate in the individual case".[67] The Guidelines on Consent under Regulation 2016/679 stipulate that when:

> "data processing is done in pursuit of several purposes, the solution to comply with the conditions for valid consent lies in granularity, i.e. the separation of these purposes and obtaining consent for each purpose".[68]

---

[63] For example, collection, storage, adaptation or alteration, retrieval, disclosure by transmission, dissemination or otherwise making available, erasure or destruction of the data subject's personal information.

[64] Guidelines on Consent under Regulation 2016/679, n 1, 5.

[65] If "the controller [NEHR authority/agency/operator] has conflated several purposes for processing and has not attempted to seek separate consent for each purpose, there is a lack of freedom". Guidelines on Consent under Regulation 2016/679, n 1, 10.

[66] Unless there is another lawful basis under GDPR, n 2, Art 6(1) that is more appropriate in the situation (see n 59); though this would be very rare in cases where controller is a public authority.

[67] Guidelines on Consent under Regulation 2016/679, n 1, 10; see also GDPR, n 2, Recital 32, "Consent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of them".

[68] Guidelines on Consent under Regulation 2016/679, n 1, 10. Valid consent may cover different operations, as long as these operations serve the same purpose.

This stipulation conforms to the requirement in Art 6(1)(a) of the GDPR that "the consent of the data subject must be given in relation to 'one or more specific' purposes and that a data subject has a choice in relation to each of them".[69]

Equally necessary for its validity under GDPR is the requirement – closely linked with the fundamental principles of lawfulness, fairness and transparency[70] – that the consent must be informed.[71] Before she agrees, or decides to exercise her right to withdraw her consent in relation processing of her personal data, either the relevant NEHR system as controller or the European Union doctor must provide Ms Drocer with the following "minimum information":[72]

(i) the controller's identity;[73]
(ii) the purpose of each of the processing operations for which consent is sought;[74]
(iii) what (type of) data will be collected and used (processing operations);[75]
(iv) the existence of the right to withdraw consent;[76]
(v) information about the use of the data for automated decision-making in accordance with GDPR Article 22 (2)(c)[77] where relevant; and
(vi) on the possible risks of data transfers to third countries (for example, Australia) due to absence of an adequacy decision and of appropriate safeguards as described in Article 46.[78]

Element (v) of the "minimum information" requirement refers to automated decision-making and/or profiling, which would be a component of most NEHR systems because they can potentially deliver such benefits as increased efficiencies, resource savings and possibility of

[69] Guidelines on Consent under Regulation 2016/679, n 1, 11.
[70] Articulated in GDPR, n 2, Art 5.
[71] Guidelines on Consent under Regulation 2016/679, n 1, 13
[72] Guidelines on Consent under Regulation 2016/679, n 1, 13–1
[73] See also GDPR, n 2, Recital 42: "For consent to be informed, the data subject should be aware at least of the identity of the controller and the purposes of the processing for which the personal data are intended."
[74] GDPR, n 2, Recital 42.
[75] See also Opinion 15/2011 of the Article 29 Data Protection Working Party on the Definition of Consent, n 11, 19–20.
[76] See GDPR, n 2, Art 7(3).
[77] See also Article 29 Data Protection Working Party (EU), Guidelines on Automated Individual Decision-making and Profiling for the Purposes of Regulation 2016/679, (adopted on 3 October 2017, last revised and adopted on 6 February 2018) 17/EN, WP251, para IV.B, 20 onwards.
[78] Pursuant to GDPR, n 2, Art 49(1)(a), which states that in "the absence of a decision pursuant to Article 45(3), a controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available"; specific information is required about the absence of safeguards described in Article 46, when explicit consent is sought. See also Opinion 15/2011 of the Article 29 Data Protection Working Party on the Definition of Consent, n 11, on the definition of consent at 19.

tailoring "services and products to align with individual needs".[79] Some of these automated decision-making processes have "the ability to make decisions [solely] by technological means without human involvement",[80] and can made with or without profiling. Article 4(4) of the GDPR defines "profiling" as:

> "any form [with or without human involvement] of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements".[81]

The Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679 classify processing operations involving profiling into "three distinct stages:

- data collection;
- automated analysis to identify correlations;
- applying the correlation to an individual to identify characteristics of present or future behaviour".[82]

The GDPR mandates that Controllers carrying out profiling meet its requirements for all three stages.[83] By stating that data subjects "shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning … [them] or similarly significantly affects… [them]", Art 22(1) of the GDPR imposes a negative injunction on controllers using these processes, unless they can demonstrate that: (1) they are necessary under certain contractual circumstances; (2) authorisation "by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests", or (3) "data subject's explicit consent".[84]

In relation to special categories of personal data, in particular health data, the controller using solely automated processing must implement safeguards for protecting the data subject's rights and freedoms and legitimate interests required by Art 9 of the GDPR.[85] If the controller is making automated decisions as described in Art 22(1), they must:

- tell the data subject that they are engaging in this type of activity;
- provide meaningful information about the logic involved; and

---

[79] Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679, n 77, 5.
[80] GDPR, n 2, Art 4.
[81] GDPR, n 2, Art 4(4).
[82] Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679, n 77, 5.
[83] Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679, n 77, 5.
[84] The phrase "explicit consent" is not defined in GDPR; however, it can be construed as an affirmative agreement that can be specifically documented by the controller.
[85] In addition, GDPR, n 2, Art 22(3) adds that these protections must include "at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision".

- explain the significance and envisaged consequences of the processing.[86]

To ensure fairness and transparency of processing,[87] the information provided to the data subject must be in accessible form, meaningful (though the controller does not need to disclose the full algorithm), and sufficiently comprehensive for the data subject to understand the reasons for the decision to use solely automatic processing and/or profiling.[88]
Failure by the controller to comply with each element of informed consent requirement will result in making the principle of user control "illusory and consent will be an invalid basis for processing" under Art 6 of the GDPR.[89]

Finally, if Ms Drocer decides to agree to the processing of her personal health data, she must explicitly indicate her consent "by a clear affirmative act".

Transfers of Personal Data to Third Countries

The sixth constituent of the "minimum information" is relevant to Ms Drocer's status as an Australian visitor to the European Union, given the probability that her EHR created in the European Union would be transferred to Australia for processing (uploading on the MHR).[90] In such cases, Art 44 of the GDPR requires that both the European Union controller and the Australian processor/controller comply with certain conditions. Significantly, Art 44 of the GDPR declares that "All provisions in this Chapter shall be applied in order to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined". This provision has been interpreted as suggesting that:

> "an application of the provisions of the GDPR relating to transfers to third countries which would be technically compliant, but which would not guarantee the level of protection for natural persons desired

> by the GDPR or the Charter of Fundamental Rights of the European Union (the Charter), would not be in conformity".[91]

Article 45(2) of the GDPR specifies some critical evaluation criteria that the European Commission[92] has to consider when "assessing the adequacy of the level of protection in a

[86] Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679, n 77, 25.
[87] GDPR, n 2, Recital 60.
[88] GDPR, n 2, Recital 58.
[89] "If the controller does not provide accessible information, user control becomes illusory and consent will be an invalid basis for processing." Guidelines on Consent under Regulation 2016/679, n 1, 13 <http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051>.
[90] The European Data Protection Supervisor in its position paper of 14 July 2014, 5 defined "transfer of personal data" as "communication, disclosure or otherwise making available of personal data, conducted with the knowledge or intention of a sender subject to the Regulation that the recipient (s) will have access to it". Cited in P Van den Bulck, "Transfers of Personal Data to Third Countries" (2017) 18 ERA Forum 229.
[91] Van den Bulck, n 90, 232.
[92] Regulation 182/2011, Art 5.

third country or international organization";[93] including "the rule of law, respect for human rights and fundamental freedoms, relevant legislation, the existence and effective functioning of one or more independent supervisory authorities and the international commitments the third country … has entered into".[94] However these general provisions:

> "regarding data protection and privacy in the third country are not sufficient. On the contrary, specific provisions addressing concrete needs for practically relevant aspects of the right to data protection must be included in the third country's or international organization's legal framework. These provisions have to be enforceable".[95]

Moreover, the European Commission's mandate is "to verify – on a regular basis – that the rules in place are effective in practice".[96]

As noted above, Australia is not on the list of countries declared by the European Commission to have an adequate data protection regime.[97] Consequently, in accordance with Art 46 of the GDPR, a controller or processor may transfer personal data to a third country "only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available".[98] In certain situations, where transfers are occasional[99] not repetitive and the data transfer is necessary for a specific purpose, Art 49(1)(a) of the GDPR allows for derogation if "the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision [by the European Commission] and appropriate safeguards". The recourse to the derogation of Art 49 of the GDPR; however, "should never lead to a situation where fundamental rights might be breached".[100]
Most probably Ms Drocer, even having been informed of the risks, would have no option but to agree to the transfer of her EHRs to Australia.[101]

---

[93] Adequacy Referential (updated), Transfers of Personal Data to Third Countries, WP 254 (adopted 28 November 2017) 3 <ec.europa.eu/newsroom/just/document.cfm?doc_id=48827>.
[94] Adequacy Referential (updated), Transfers of Personal Data to Third Countries, n 93, 3.
[95] Adequacy Referential (updated), Transfers of Personal Data to Third Countries, n 93, 4.
[96] Adequacy Referential (updated), Transfers of Personal Data to Third Countries, n 93, 3; GDPR, n 2, Art 45(4).
[97] Third countries given adequacy status include Andorra, Argentina, Canada, Guernsey, Isle of Man, Israel, Jersey, New Zealand, Switzerland, Uruguay, and the United States. Australia has a bilateral agreement with the European Union Commission with regards to the sending of air passenger data and the use of financial data (Data and Terrorist Finance Tracking Programme (TFTP)); however, neither agreement covers EHRs.
[98] GDPR, n 2, Art 40(3) specifies that one of the methods for providing appropriate safeguards is a binding and enforceable commitment by the controller or processor to a code of conduct. The Code of Conduct on eHealth, which is being developed, will include the obligation in GDPR, n 2, Art 7(1) that the data controller should be able to demonstrate the data subject's affirmative consent. See, Letter of the Chair of the Article 29 WP to mHEALTH (11 April 2018) <http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=625391>.
[99] GDPR, n 2, Recital 111.
[100] Guidelines on Article 49 of Regulation 2016/679, WP 262 (adopted 6 February 2018) 3.
[101] Other GDPR rules might also provide grounds for data transfers in the absence of adequacy certification.

V. Australian Legislative Framework for MHR System and Patients' Consent to Processing of Their Personal Data

What is the nature and role of consent under MHR scheme? How do rights and protections provided to data subjects under GDPR compare with those under MHR legislative framework?

(2018) 26 JLM 23 at 34

Let us assume that before leaving for the European Union, Ms Drocer followed the advice of her general practitioner who advised her to register for MHR. The general practitioner might or might not have informed her that the particular general practice was in receipt of the Practice Incentives Program (eHealth Incentive) – neither provisions and guidelines of the MHR legislative framework, nor any other instruments seem to mandate such disclosure and the concomitant conflict of interests.

Australia's NEHR system, MHR,[102] is directly[103] governed by three statutes: *My Health Records Act 2012* (Cth), *Healthcare Identifiers Act 2010* (Cth),[104] the relevant provisions of the *Privacy Act 1988* (Cth),[105] six legislative instruments: the Healthcare Identifiers Regulations 2010 (Cth),[106] My Health Records Regulation 2012 (Cth),[107] My Health Records (Assisted Registration) Rule 2015 (Cth),[108] My Health Records (Information Commissioner

---

[102] Mendelson and Wolf, "Privacy and Confidentiality", n 14, Ch 14, 266–282; Mendelson and Wolf, "'My [Electronic] Health Record' – Cui Bono (for Whose Benefit)?", n 13.

[103] Other legislation applicable to the *My Health Records Act 2012* (Cth) includes: *National Health Reform Act 2011* (Cth); *Private Health Insurance Act 2007* (Cth); *National Health Security Act 2007* (Cth); *Health Insurance Act 1973* (Cth); *Census and Statistics Act 1905* (Cth); *National Health Act 1953* (Cth); *Australian Bureau of Statistics Act 1975* (Cth); *Freedom of Information Act 1982* (Cth); *Privacy Amendment (Private Sector) Act 2000* (Cth); *Human Services Legislation Amendment Act 2011*(Cth); *Australian Institute of Health and Welfare Act 1987* (Cth); *Australian Information Commissioner Act 2010* (Cth)

[104] The *Healthcare Identifiers Act 2010* (Cth) ss 3, 9 enables assignment of a unique identifying number (Healthcare Identifier) to each health care organisation (entity), each individual health care provider, and each health care recipient (patient) thus "ensuring that an entity that provides, or an individual who receives, healthcare is correctly matched to health information that is created when healthcare is provided".

[105] The *Privacy Act 1988* (Cth) regulates the handling of personal information by the System Operator and all private sector healthcare provider organisations.

[106] The Healthcare Identifiers Regulations 2010 (Cth) provide additional detail and requirements regarding the operation of the Healthcare Identifiers Service. Australian Digital Health Agency, My Health Record, Legislation and Governance <https://www.myhealthrecord.gov.au/about/legislation-and-governance>

[107] The My Health Records Regulation 2012 (Cth) "prescribe requirements for access control mechanisms, identity verification, the handling of specified types of records and participation requirements, including security requirements for healthcare provider organisations".

[108] The My Health Records (Assisted Registration) Rule 2015 (Cth) specifies requirements for registered healthcare providers that assist individuals to register through "assisted registration" procedures. Australian Digital Health Agency, n 106.

Enforcement Powers) Guidelines 2016 (Cth),[109] My Health Records Rule 2016 (Cth)[110] and My Health Records (National Application) Rules 2017 (Cth) which has enabled the government to change the previous "opt-in", consent-based electronic records system to an opt-out model under Sch 1 of the *My Health Records Act 2012* (Cth). The Framework to Guide the Secondary Use of My Health Record System Data (2018)[111] governs the MHR Secondary Use of Data Governance Board "when making decisions about granting access to, and making available, MHR system data for secondary use".

The three statutes, Rules, Regulations and Guidelines are in parts opaque,[112] with complex interactions among them, including overlaps. For example, "any breach of *My Health Records Act 2012*, in connection with health information included in a healthcare recipient's My Health Record is an 'interference with privacy of the healthcare recipient' for the purposes of the *Privacy Act*."[113] However, "disclosure of personal information that is otherwise prohibited under the *Privacy Act* is allowable if it is required by the *My Health Records Act*".[114]

The MHR scheme authorises Digital Health Agency as the System Operator[115] to collect, use and disclose[116] health information contained in an individual's MHR record.[117] In relation to data processing, s 13A(1) of the *My Health Record Act 2012* (Cth) empowers the System Operator to "arrange for the use, under the System Operator's control, of computer programs [algorithms] for any purposes for which the System Operator may make decisions under this

---

[109] The My Health Records (Information Commissioner Enforcement Powers) Guidelines 2016 (Cth) direct "the Information Commissioner's general approach to exercising its enforcement and investigative powers under the My Health Record system". Australian Digital Health Agency, n 106.

[110] The My Health Records Rule 2016 (Cth) specifies requirements for registered entities in the system. Australian Digital Health Agency, n 106.

[111] Framework to Guide the Secondary Use of My Health Record System Data (May 2018) 3.

[112] See, eg, My Health Records (National Application) Rules 2017 (Cth).

[113] Guide to Mandatory Data Breach Notification in the My Health Record System (October 2017).

[114] Guide to Mandatory Data Breach Notification in the My Health Record System, n 113.

[115] Under contract with the System Operator, a private company, Accenture Australia Holdings Pty Ltd (a subsidiary of Accenture Holdings plc), acts as the National Infrastructure Operator of the system. Accenture provides and manages the National Repositories Service database system, "which holds the key data sets which make up a My Health Record, including shared health summaries, event summaries, discharge summaries, specialist letters, consumer entered health summaries and consumer notes".

[116] Neither "collection" nor "disclosure" is defined in the legislation; however, according to *My Health Record Act 2012* (Cth) s 5, the verb "use" includes "accessing the information; viewing the information; modifying the information and deleting the information"

[117] *My Health Records Act 2012* (Cth) s 58. Other registered repository operators (entities that hold, "or can hold, records of information included in My Health Records for the purposes of the My Health Record system") and portal operators (operators of an electronic interface that facilitates access to the My Health Record system); as well as the Chief Executive Medicare, the Department of Veterans' Affairs, the Department of Defence and the department for responsible for aged care can collect use and disclose identifying information. *My Health Records Act 2015* (Cth) ss 5, 49, 50D, 58A.

Act". By virtue of s 13A(2), "[a] decision made by the operation of a computer program under an arrangement made under subsection (1) is taken to be a decision made by the System Operator".[118]

It is unclear whether the System Operator's "computer programs" are used for profiling, and what are the kinds of System Operator's decisions are based on what from the wording of s 13A(2) appear to be solely automated processing of personal health information.

The MHR legislation uses term "personal information" as defined s 6 of the *Privacy Act 1988*, namely "Information or an opinion about an identified individual, or an individual who is reasonably identifiable: (a) whether the information or opinion is true or not; and (b) whether the information or opinion is recorded in a material form or not". It also adopts "health information",[119] which s 6FA of the *Privacy Act 1988* defines as including, amongst others: "information or an opinion about: the health, including an illness, disability or injury, (at any time) of an individual; an individual's expressed wishes about the future provision of health services to the individual"; information about a health service provided, or to be provided; "personal information collected in connection with the donation, or intended donation, by an individual of his or her body parts, organs or body substances"; and "genetic information about an individual in a form that is, or could be, predictive of the health of the individual or a genetic relative of the individual".[120]

When initially enacted as the Personally Controlled Electronic Record scheme,[121] what is now the MHR scheme was an "opt-in" model, whereby competent adult "healthcare recipients" – patients, also referred to as "customers"[122] – had to register in order to get their health records uploaded on the system. According to the Office of Australian Privacy Commissioner's Privacy Fact Sheet 20 titled “Consent and the Handling of Personal Information in Your My Health Record” (March 2016), in order to be valid, the consent to register on the system the registrant had to be "be adequately informed before giving consent", it had to be "provided voluntarily", "current and specific" and the person had to have "the capacity to understand and communicate … consent".[123] These requirements reflect the

[118] Patients can set "advanced access controls" to restrict the nominated representatives and healthcare provider organisations from accessing their MHRs, and their access to particular records within them. *My Health Records Act 2012* (Cth) ss 15(b)(i), (c); My Health Records Rule 2016 (Cth) r 4 (definition of "advanced access controls").

[119] *My Health Records Act 2015* (Cth) s 5.

[120] *Privacy Act 1988* (Cth) s 6FA.

[121] *Personally Controlled Electronic Health Records Act 2012* (Cth) was amended and re-named in 2016 as *My health Records Act 2012* (Cth). For a discussion of patients' "personal control" of their records, see Mendelson and Wolf, '"My [Electronic] Health Record' – Cui Bono (for Whose Benefit)?", n 14.

[122] For an excellent critique of policies that underpin MHR system see, CM Showell, "Citizens, Patients and Policy: A Challenge for Australia's National Electronic Health Record" (2011) 40 Health Information Management Journal 39.

[123] Office of the Australian Information Commissioner, Privacy Fact Sheet 20: Consent and the Handling of Personal Information in Your My Health Record <https://www.oaic.gov.au/individuals/privacy-fact-sheets/health-and-digital-health/privacy-fact-sheet-20-consent-and-the-handling-of-personal-information-in-your-my-health-record>

Australian Privacy Principles;[124] however, the matter of valid consent to registration on MHR system is now moot.

The My Health Records (National Application) Rules 2017, issued by Mr Greg Hunt, Minister for Health, on 30 November 2017, changed the system to an opt-out operation "so that consumers will automatically get a MHR, unless they choose not to have one".[125] People who did not wish to have a MHR created on their behalf have an opportunity to "opt out" during the short period running from 16 July to 15 November 2018.[126]

On the Australian Digital Health Agency's MHR website there is no easily accessible information about the nature (automated, solely automated processing) and purposes (profiling) of the System Operator's processing operations that would enable the data subject to understand the reasons for its decision to use these processing techniques when choosing whether to opt out. Australians who do not opt out during the specified period, are automatically registered in the MHR system. Under GDPR, this kind of "consent" to automatic registration on the system designed to process their personal data by silence or inactivity would be considered a flagrant breach of Art 6(1).

However, even people who intend to opt out have had their personal data processed without consent. This is because, following registration of the My Health Records (National Application) Rules 2017 on the Federal Register of Legislation (1 December 2017),[127] Sch 1 of Pt 2 (the "opt-out model") of the *My Health Records Act 2012* came into operation, with r 5 of the My Health Records (National Application) Rules 2017 authorising "the System Operator to collect information about people ['all healthcare recipients in Australia'] who [were] not registered in the MHR system as part of preparation for the implementation of opt-out".[128]
The non-consensually collected "preparatory" information[129] comprised every person's name, address, date of birth and gender; if applicable, the Medicare number and/or the Veterans' Affairs Department file number. In addition, by virtue the cl 1.1.7 of the My Health Records Regulation 2012 (Cth),[130] the System Operator also collects such "preparatory" identifying information as personal telephone number; personal electronic address; and whether each person's identity has been verified. In relation to identity verification, the System Operator collects details of "particular form of identification document (such as a driver's licence or passport)", which include "(i) the document number; and (ii) the State or Territory in which

[124] See *Privacy Amendment (Enhancing Privacy Protection) Act 2012* (Cth) Sch 1.
[125] My Health Records (National Application) Rules 2017 (Cth).
[126] My Health Records (National Application) Rules 2017 (Cth) r 6; the Australian Digital Health Agency, Find More about Opt-Out <https://www.myhealthrecord.gov.au/for-you-your-family/howtos/opt-out>.
[127] My Health Records (National Application) Rules 2017 (Cth) were registered on 1 December 2017, and tabled in the House of Representatives and the Senate on the 4 and 5 December 2017 respectively.
[128] The authority for the collection is provided by the *My Health Record Act 2012* (Cth) Sch 1 cl 8(1) Item 1; Explanatory Statement Issued by Authority of the Minister for Health, *My Health Records Act 2012* (Cth); My Health Records (National Application) Rules 2017 (Cth).
[129] The MHR legislation distinguishes between information about individuals before they are registered and "health information for the purposes of a healthcare recipient's My Health Record". My Health Records (National Application) Rules 2017 (Cth) r 7.
[130] Pursuant to *My Health Record Act 2012* (Cth) s 9(3)(i).

the document was issued; and (iii) the name of the entity that issued the document". Neither Ms Drocer, nor any other Australian health care recipient, has been given the right to consent to, refuse, or restrict this processing of their personal data. Such processing might be legal under Australian law, but would not be legitimate under GDPR.

*The "Standing" or "Ongoing" Consen*t

Perhaps the most concerning approach of the MHR regulatory framework is its peculiar notion of "standing" or "ongoing" consent. When Ms Drocer registered for a My Health Record,[131] she probably did not realise that the registration required her:

> "to give a standing, or ongoing, consent to records containing … [her] health information being uploaded to … [her] record by healthcare providers involved in … [her] care".[132]

The importance of valid consent in protecting fundamental rights of European Union data subjects, and extensive definitions of its core elements in the GDPR have been discussed above. In contrast, the *My Health Record Act 2012* does not define consent at all, and according to the circular definition in s 6 of the *Privacy Act 1988* "consent means express consent or implied consent".

Instead, the MHR scheme has created a notion of "standing" or "ongoing" consent. These terms are not used in the MHR legislation and subordinate legislation, nor do they appear in the Office of the Australian Information Commissioner's "'Key Concepts' for the Australian Privacy Principles Guidelines" (April 2015). It appears that the notion of such "standing/ongoing" consent somehow derived from the following s 41(3), 41(3A) and 41(4) of the *My Health Record Act 2012*:

> "(3) The System Operator is not required to register a healthcare recipient if the healthcare recipient does not consent to a registered healthcare provider organisation uploading to the My Health Record system any record that includes health information about the healthcare recipient,[133]
> (3A) A registered healthcare provider organisation[134] is authorised to upload to the My Health Record system a record in relation to a healthcare recipient (the patient) that includes health information about another healthcare recipient (the third party), if the health information about the third party is directly relevant to the healthcare of the patient, subject to a law of a State or Territory that is prescribed by the regulations for the purposes of subsection (4).
> (4) A consent referred to in subsection (3), and an authorisation given under subsection (3A), have effect despite a law of a State or Territory that requires consent to the disclosure of particular health information: (a) to be given expressly; or (b) to

[131] *My Health Records Act 2015* (Cth) ss 39, 40.
[132] Office of the Australian Information Commissioner, n 123.
[133] This is subject to: "(a) express advice given by the healthcare recipient to the registered healthcare provider organisation that a particular record, all records or a specified class of records must not be uploaded; (b) a law of a State or Territory that is prescribed by the regulations for the purposes of subsection (4)".
[134] For example, state and territory health departments, hospitals, medical practices, pathology, radiology laboratories, pharmacies, allied health practitioners practices, etc

> be given in a particular way; other than a law of a State or Territory prescribed by the regulations for the purposes of this subsection."[135]

It appears that what is the right by the health care recipients not to consent to uploading to the MHR system records with their personal health information in s 41(3) becomes consent in s 41(4) on the basis that unless patients affirmatively refuse the processing, their non-refusal is taken to be a "standing" or "ongoing" consent. The Australian Digital Health Agency on the website titled "Digital health and patient consent" states that:

> "In registering for a My Health Record, patients provide a "standing consent" for all healthcare organisations involved in their care to upload clinical information to their record. *There is no requirement for a provider to obtain consent on each occasion prior to uploading clinical information*. There is also no requirement for a patient to review clinical information prior to it being uploaded."[136]

This approach is contrary to all GDPR principles that protect data subjects' fundamental rights to control their data through exercising their right to consent or refusal of having their data processed. It infringes each GDPR requirement for legitimate personal data processing under Art 6.

Inverting the requirement of data subjects' valid consent for uploading their personal health data into a right to refuse such processing relieves a health care provider as the processor from the responsibility of explaining to the data subject-cum-patient such matters as the controller's identity, the purpose of each of the processing operations, the kind of personal health information that is going to be uploaded,

the potential use of the data for automated decision-making, and the existence of the right to withdraw consent.[137] This right exists under s 51(1) of the *My Health Record Act 2012*, which requires the System Operator in writing[138] "to decide to cancel or suspend the registration of a healthcare recipient … if the healthcare recipient … requests the System Operator, in writing, to cancel or suspend the registration".[139]

---

[135] Under My Health Record Regulation 2012 (Cth) 3.1.1 (emphasis in the original), prescribed laws are *Public Health Act 2010* (NSW) ss 56, 92; *Public Health Act 2005* (Qld) ss 55, 77–79, 105–107, 175–177, 220–222, 238–240, 266–268; *Public Health Act 1997* (ACT) ss 110, 111.

[136] Australian Government, Australian Digital Health Agency, Understand When You Can View and Upload Information <https://www.digitalhealth.gov.au/using-the-my-health-record-system/maintaining-digital-health-in-your-practice/patient-consent> (emphasis in the original).

[137] According to the Australian Digital Health Agency's "Digital health and patient consent" website, "the Australian Medical Association's Guide to Using the My Health Record, s 4.5 advises medical practitioners that 'it is good medical practice to advise a patient that you will be uploading information to their My Health Record, particularly if this information might be considered sensitive'" <https://www.digitalhealth.gov.au/using-the-my-health-record-system/maintaining-digital-health-in-your-practice/patient-consent>.

[138] Australian Digital Health Agency, Cancel My Record <https://www.myhealthrecord.gov.au/for-you-your-family/howtos/cancel-my-record>.

[139] Subsequent to cancellation, while health care providers will be barred from uploading or accessing the patient's MHR; data contained in it is to be kept for a period of 30 years after the patient's death or, if the date of death is unknown, for a period of 130 years after the date

Finally, in accordance with authorisation provided in s 41(3A), with the exception of New South Wales, Queensland and the Australian Capital Territory, health care providers in Australia can lawfully upload, and thereby disclose, on the MHR system record health information about a third party if it "is directly relevant to the healthcare of the patient". Apart from undefined "direct" relevance (which does not reflect any of six lawful grounds for processing of personal data under Art 6 of the GDPR), there are no legislative restrictions imposed on the nature, sensitivity and volume of the health information authorised to be uploaded without consent of either party.

Familiar with the GDPR principles, Ms Drocer might well be dismayed and appalled by the treatment of data subjects' right to consent under the MHR regime, and so should other Australians. Australia might not be seeking certification for attaining adequate level of data protection; however, if the government were to do so, laws and regulations relating to consent would have to be changed in line with GDPR.

---

of birth. During this period My Health Record may be accessed by the System Operator for the purposes of maintenance, audit and other purposes required or authorised by law.