Singapore Journal of Legal Studies
[2021] 56–75

WHOSE HEALTH RECORD? A COMPARISON OF PATIENT RIGHTS UNDER NATIONAL ELECTRONIC HEALTH RECORD (NEHR) REGULATIONS IN EUROPE AND ASIA-PACIFIC JURISDICTIONS

JAMES **SCHEIBNER**,* MARCELLO **IENCA**** and EFFY **VAYENA*****

In this paper, we compare four patient rights regarding data stored in NEHRs under nine European and Asia-Pacific jurisdictions. We aim to ascertain whether the success and failure of NEHR implementations could be attributable to differences in patient rights. We note that while there is a convergence of access controls, there is a divergence with respect to controlling third-party access and modifying patient data. Analysing these divergences through four bioethical principles defined by Beauchamp and Childress, we find claims of patient empowerment mask a neoliberal perspective of outsourcing responsibility to patients. Likewise, refusing sufficient granular control can contribute to patient mistrust. We argue that it is important to conceptualise NEHRs as a public good and design regulatory frameworks accordingly.

I. INTRODUCTION

Electronic health records ("EHRs") are no longer just a mechanism for conveniently storing patient data. Governments, healthcare providers and researchers all hunger for more data to help solve the "wicked problems" posed by healthcare. These include ageing populations, chronic illness and fragmented healthcare delivery.[1] Advocates for reform argue that electronically storing and making patient EHRs available can help fix the "wicked problems" of healthcare management.[2] It is therefore tempting to

* Lecturer, College of Business, Government and Law, Flinders University, Australia. Postdoctoral Research Fellow, Health Ethics and Policy Laboratory, Department of Health Sciences and Technology, ETH Zürich, Switzerland.

** Senior Research Fellow, Health Ethics and Policy Laboratory, Department of Health Sciences and Technology, ETH Zürich.

*** Chair of Bioethics, Health Ethics and Policy Laboratory, Department of Health Sciences and Technology, ETH Zürich, email: <effy.vayena@hest.ethz.ch>. The authors would like to thank Agata Ferretti for her helpful suggestions and comments on drafts of this manuscript.

1 Sara E Shaw & Rebecca Rosen, "Fragmentation: A wicked problem with an integrated solution?" (2013) 18:1 Journal of Health Services Research & Policy 61 at 64.

2 Yakov Flaumenhaft & Ofir Ben-Assuli, "Personal health records, global policy and regulation review" (2018) 122:8 Health Policy 815 at 816 [Flaumenhaft & Ben-Assuli]; Effy Vayena *et al*, "Element of a New Ethical Framework for Big Data Research" (2016) 72:3 Wash & Lee L Rev Online 423 at 423.

conclude these benefits would be amplified by nationally coordinated EHR systems.[3] However, a lack of organisational connectedness between the relevant stakeholders creates a "garbage can" decision-making style approach to reform. Responding to crises, policy advocates proffer "solutions to ill-defined problems and answers to unasked questions", leading to reactive responses and repetitive policy failures.[4] In particular, in practice national electronic health record ("NEHR") implementations have emerged as "paradigm cases of public policy failure", becoming wicked problems themselves.[5] Whilst NEHRs in England and France stand as testament to these failures,[6] implementations in other countries, such as Estonia and Denmark, have flourished.[7] In this paper, we attempt to identify factors that delineate whether NEHR implementations succeed or fail by constructing a typology of patient rights under NEHR regulations. Specifically, we assess whether legislative or policy instruments to protect patient rights, along with guarantees of security and legitimacy, are associated with the success of NEHRs.[8] We seek to contribute to the debate between the broader societal uses of NEHRs and the rights of patients over their data.[9]

Accordingly, our paper compares NEHR implementation strategies in nine jurisdictions from Europe and the Asia-Pacific. We examine these implementation strategies to determine whether there is an international convergence of norms concerning the rights of patients in NEHR systems. To answer these questions, our paper is split into four sections. In the first section, we define our methodological approach for comparing NEHR implementation strategies and creating a typology of different patient rights. In the second section, we divide our sample of countries into three subcategories. First, we consider countries that have a NEHR, implementation strategy and specific supporting legislation (Australia, Estonia and Italy). Secondly, we include countries that have a NEHR system and an implementation strategy but do not have specific supporting legislation (Denmark, Singapore and Spain). Finally, we examine countries that have a NEHR implementation strategy, but no NEHR or legislation (Germany, New Zealand and Switzerland). In the third section, we analyse the rights available in each country to determine whether there has been a convergence or a divergence of rights. We analyse each of these privacy rights along several dimensions. In the fourth section, we determine the ethical and legal effects of these convergences and divergences by reference to the four principles of

---

3 Zoe Morrison *et al*, "Understanding Contrasting Approaches to Nationwide Implementations of Electronic Health Record Systems: England, the USA and Australia" (2011) 2:1 Journal of Healthcare Engineering 25 at 26 [Morrison].

4 Calum Paton, "Garbage-can Policy-making Meets Neo-liberal Ideology: Twenty Five Years of Redundant Reform of the English National Health Service" (2014) 48:3 Social Policy & Administration 319 at 320.

5 Karin Garrety *et al*, "National electronic health record systems as 'wicked projects': The Australian experience" (2016) 21:4 Information Polity 1 at 2-3 [Garrety *et al*].

6 Simon de Lusignan & Bridgette Seroussi, "A comparison of English and French approaches to providing access to Summary Care Records" (2013) 186 Studies in Health Technology and Informatics 61 at 64.

7 DA Ludwick & John Doucette, "Adopting electronic medical records in primary care: Lessons learned from health information systems implementation experience in seven countries" (2009) 78 International Journal of Medical Informatics 22 at 29 [Ludwick & Doucette].

8 Anton Vedder *et al*, "The Law as a 'Catalyst and Facilitator' for Trust in E-Health: Challenges and Opportunities" (2014) 6:2 Law, Innovation and Technology 305 at 308.

9 Karin Garrety *et al*, "National electronic health records and the digital disruption of moral orders" (2014) 101 Social Science & Medicine 70 at 74.

biomedical ethics. We conclude there are two points of divergence most likely to lead to failure (as defined by a lack of public acceptance and patient uptake). These points are a lack of patient control over how third parties use their EHRs and confusion over patient responsibility for the information stored in NEHRs. Both are symptomatic of a neoliberal approach to EHR management that outsources informational responsibility to patients, engendering mistrust in both patients and doctors. Accordingly, an adaptive patient rights approach underpinned by conceptualising NEHRs as a public good is necessary for these implementation strategies to achieve widespread public support.

II. Methodology

A. *Methodological Background*

We use a comparative approach to legislative analysis based on the concept of a legal typology, otherwise referred to as a legal taxonomy. Sherwin names early common law privacy evolving from tort and contract law as an example of a legal typology.[10] Similarly, EHR regulations have emerged from overlapping laws, including privacy and data protection, medical professional regulation and administrative law. Mattei argues legal taxonomies can also be used to describe how laws are transferred between jurisdictions.[11] Mattei also notes legal taxonomies can define different legal concepts within a particular jurisdiction or in a particular field of law.[12] Likewise, Solove uses legal taxonomy to examine different uses of information processing under US law.[13] These include aggregation, identification, insecurity, secondary use and exclusion.[14] Solove then connects these uses to the relevant privacy harms, including breaches of confidentiality, disclosure, exposure, increased accessibility, compromise, appropriation and distortion.[15] Solove considers this typology with respect to the potential uses (and misuses) of EHR systems, as well as the public policy interests associated with patient privacy.[16] In addition, Voss and Castets-Renard use legal taxonomy to consider how different jurisdictions conceptually approach the "right to be forgotten".[17] We refer to these categories when considering how patients can erase their data from NEHRs. Finally, Koops *et al* use legal taxonomy to compare constitutional concepts of privacy in North America and Europe.[18] In

---

10 Emily Sherwin, "Legal Taxonomy" (2009) 15:1 Legal Theory 25 at 27, 31.

11 Ugo Mattei, "Three Patterns of Law: Taxonomy and Change in the World's Legal Systems" (1997) 45:1 Am J Comp L 5 at 6-7.

12 *Ibid* at 6.

13 Daniel J Solove, "A Taxonomy of Privacy" (2005-2006) 154:3 U.Pa.L.Rev. 477 at 484-491 [Solove].

14 *Ibid* at 506.

15 *Ibid* at 525.

16 See *Sorrell, Attorney General of Vermont et al v IMS Health Inc et al* (2011) 131 S. Ct. 2653 at 2682 (citing Solove, *ibid*); Sebastian Porsdam Mann, Julian Savulescu & Barbara J Sahakian, "Facilitating the ethical use of health data for the benefit of society: electronic health records, consent and the duty of ease rescue" (2016) 374:2083 Philosophical Transactions of the Royal Society A 20160130 at 3 [Mann, Savulescu & Sahakian].

17 Gregory W Voss & Celine Castets-Renard, "Proposal for an International Taxonomy on the Various Forms of the Right to be Forgotten" (2015-2016) 14:2 Colorado Technology Law Journal 281 at 287-299.

18 Bert-Jaap Koops *et al*, "A Typology of Privacy" (2016-2017) 38:2 University of Pennsylvania Journal of International Law 483 at 504-510 [Koops *et al*].

the next section, we explain how we developed a legal taxonomy of different patient rights associated with NEHRs.

B. *Jurisdiction Selection*

As part of this study, to inform our selection we first examined the literature on NEHRs.[19] We selected jurisdictions in Europe and the Asia-Pacific region purposively. Specifically, we selected those belonging to the Organisation for Economic Cooperation and Development ("OECD") that had previously answered the World Health Organization ("WHO") eHealth Observatory Global Survey. As OECD member states, each of these jurisdictions have equivalent spending capacity for healthcare programs. Therefore, in our sample, there are no significant economic disparities between nations that could lead to resource constraints and subsequent lack of implementation progress. We did so to avoid generalising our results based only on the findings from high-income countries.[20]

Further, a significant portion of the literature examining NEHR implementation has focused on two countries; the United Kingdom ("UK") and the United States ("US"). As Coiera notes, these countries have adopted contrasting "top-down" and "bottom-up" approaches to implementing NEHRs. Adler-Milstein and Jha argue high rates of meaningful EHR use following the Health Information Technology for Economic and Clinical Health ("HITECH") Act could be instructional for other developed nations.[21] On the other hand, the HITECH Act has been criticised for failing to encourage interoperability between hospitals.[22] Further, following the approach to international legal taxonomies, we argue other jurisdictions can also offer reciprocal guidance on designing EHR regulations. Therefore, we sought to examine jurisdictions outside these two countries.

Finally, advances in European data protection laws, including the EU General Data Protection Regulation ("*GDPR*") and the modernised Convention 108, have extended patient rights.[23] The literature published so far has compared the *GDPR*

---

19 Enrico Coiera, "Building a National Health IT System from the Middle Out" (2009) 16:3 Journal of the American Medical Informatics Association 271 at 271-273 [Coiera]; Ludwick & Doucette, *supra* note 8 at 25; Morrison, *supra* note 4 at 27-30; OECD, *Strengthening Health Information Infrastructure for Health Care Quality Governance* (Paris: OECD Health Policy Studies, OECD Publishing, 2013) [OECD]; Flaumenhaft & Ben-Assuli, *supra* note 3 at 816.

20 Julia Adler-Milstein *et al*, "Benchmarking health IT among OECD countries: better data for better policy" (2014) 21:1 Journal of the American Medical Informatics Association 111 at 112.

21 Julia Adler-Milstein & Ashish K Jha, "HITECH Act Drove Large Gains in Hospital Electronic Health Record Adoption" (2017) 36:8 Health Affairs 1416 at 1421-1422.

22 Leonidas L Fragidis & Prodromos D Chatzoglou, "Implementation of a nationwide electronic health record (EHR): The international experience in 13 countries" (2018) 31:2 International J Health Care QA 116 at126.

23 EC, *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)*, [2016] OJ, L119/1 [*GDPR*]; *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data,* 28 January 1981, ETS 108 (entered into force 1 October 1985); *Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, 17 May 2018, CETS 223.

as a supranational instrument relative to other national regulations.[24] By contrast, we explore and compare the national derogations of the *GDPR* and Convention 108, along with other legislation relevant to EHRs. Under EU and European data protection law, government health departments and healthcare providers should respect fundamental principles of data protection law when designing NEHR systems.[25] Further, collecting health-related data for an EHR should be considered the primary purpose of data processing. Any other subsequent processing should be considered a secondary purpose for which explicit and informed consent must be sought.[26] Nevertheless, the purpose of European data protection law is to protect the rights of individuals, not to establish a legislative framework for managing EHRs.[27] Therefore, we considered additional national measures and legislation for regulating EHRs where they exist.[28] Although not currently signatories to Convention 108, this Convention and the *GDPR* have influenced recent reform in the Asia-Pacific.[29]

We first started with three countries that have adopted NEHRs, along with a NEHR strategy and implementing legislation—Australia, Italy and Estonia. We then complemented these countries with NEHRs and NEHR strategies, but no underpinning legislation—Denmark, Spain and Singapore. Thirdly, we selected countries that have a NEHR strategy or legislation but do not have a NEHR and either legislation or a strategy—Germany, New Zealand and Switzerland. We also chose these jurisdictions as they have attempted to implement three different types of NEHR architecture—centralised, decentralised and personally controlled.[30] To compare the impact of regimes and architectures on patient rights, we first started by examining the relevant statutes in each jurisdiction, along with case law and other secondary materials such as journal articles and book chapters. We developed four patient rights from the 2015 WHO eHealth Observatory Survey[31] as follows:

1. Allows individuals electronic access to their own health-related data when held in an EHR;
2. Allows individuals to specify which health-related data from their EHR can be shared with health professionals of their choice;

---

24 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) 26:1 Journal of Law, Medicine & Ethics 23.

25 Article 29 Data Protection Working Party, *Working Document on the processing of personal data relating to health in electronic health records (EHR)*, EC Working Document WP 131 (15 February 2007), online: EC <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp131_en.pdf> at 6-7 [Article 29 Data Protection Working Party].

26 *Ibid* at 7.

27 *Ibid* at 21.

28 Mary Rogan, "Improving Criminal Justice Data and Policy" (2012) 43:2 Economic and Social Review 303 at 311.

29 Graham Greenleaf, "Global Data Privacy Laws 2019: 132 National Laws & Many Bills" (2019) 157:1 Privacy Laws & Business International Report 14 at 17.

30 Article 29 Data Protection Working Party, *supra* note 25 at 21.

31 See WHO, *Third Global Survey on eHealth—2015*, online: WHO <https://www.who.int/goe/survey/2015survey/en/>.

3. Allows individuals electronic access to their own health-related data when held in an EHR if it is inaccurate; and
4. Allows individuals to demand the deletion of health-related data from their EHR

We considered the extent of each of these rights in each jurisdiction as well; that is, whether they offered full or partial rights for patients. For this analysis, we accessed any legislation or policies directly referred to in WHO e-Health Observatory, OECD, European Commission or other government reports. Further, we used secondary materials to purposively identify other legislation from our selected jurisdictions. We first searched government websites to identify any English translations of legislation. For documents with no English translation, we used online translation services (such as DeepL[32] or Google Translate[33]). We could not verify the accuracy of our machine translations where no English version was available. Instead, we compared our translations with official English government translations in other jurisdictions where available to ensure the accuracy of our methods.[34] The relevant legislation is disclosed in Table 1 below.

Table 1 Legislation, regulations and strategies governing NEHR implementations in nine jurisdictions.

Jurisdiction	***Legislation***	***Strategies***
Australia	*MyHealth Records Act 2012* (Cth); *MyHealth Records Rules 2016* (Cth); *Health Identifiers Act 2010* (Cth); and *Privacy Act 1988* (Cth).	Framework to guide the secondary use of My Health Record system data.
Estonia	*Statute of the Health Information System 2016*; *Regulation on System of Security Measures for Information Systems, No 252, 2007*; *Personal Data Protection Act 2018*, repealing *Personal Data Protection Act 2007*; and *Health Services Organisation Act 2001*.	The Health Information System Development Plan, Estonian Ministry of Social Affairs, 2004; and The Health Information Systems Development Plan, Estonian Ministry of Social Affairs, 2008.

[32] DeepL, online: DeepL <https://www.deepl.com/home>.
[33] Google Translate, online: Google Translate <https://translate.google.com>.
[34] Jonathan Fox, "Out of Sync: The Disconnect Between Constitutional Clauses and State Legislation on Religion" (2011) 44:1 Canadian Journal of Political Science 59 at 63.

Table 1 (*Continued*)

Jurisdiction	*Legislation*	*Strategies*
Italy	*Harmonization Decree* (Legislative Decree 19 September 2018, No 101), amending *Personal Data Protection Code* (Legislative Decree 30 June 2003, No 196); *Digital Administration Code* (Legislative Decree 7 March 2005, No 82); and Legislative Decree 17 December 2012, No 221.	Guidelines on the Electronic Health Record and the Health File 2009; National Health Information Strategy 2011; and Additional regulations provided by autonomous regions.
Denmark	*Data Protection Act 2018*, replacing *Danish Act on Processing of Personal Data* (Act No 428 of 31 May 2000); *Archive Act* (Consolidated Act No 1201 of 28 September 2016 on Archives); *Consolidated Act No 1083 of 15 September 2017 on Research Ethics Review of Health Research Projects* (Research Ethics Review Act); *Health Act* (Consolidated Act No 191 of 28 February 2018 on Health); Consolidated Act No 903 of 26 August 2019 on Executive Order of the Health Act; and Executive Order of the Danish Medicines Agency's electronic registration of individual citizens' medical information 2011	Danish Action Plan for EHRs 1996; Danish National Strategy for IT in the Hospital Sector 2000-2002; Danish National Strategy for IT in Healthcare 2002; Danish National Strategy for IT in Healthcare 2003-2007; Danish National Strategy for IT in Healthcare 2008-2012; and Code of Conduct for Research Integrity 2015.
Singapore	*Personal Data Protection Act 2012*; *Human Biomedical Research Act 2015*; and *Healthcare Services Bill 2018*.	Medical Council Guidelines.
Spain	*General Health Act* (Law 14/1986 of 25 April); *Patient Rights Act* (Law 41/2002 of 14 November);	Royal Decree 4/2010 of 8 January, which regulates the National Interoperability Framework within the e-government scope; and

Table 1 (*Continued*)

Jurisdiction	***Legislation***	***Strategies***
	National Health Service Quality Act (Law 16/2003 of 27 May); *Citizens' Electronic Access to Public Services Act* (Law 11/2007 of 22 June); *Biomedical Research Act* (Law 14/2007 of 3 July); *General Public Health Act* (Law . 33/2011 of 4 October); *Protection of Personal Data and the Guarantee of Digital Rights Act* (Law 3/2018 of 6 December), repealing Law 15/1999 of 13 December on Personal Data Protection	Coordination with Autonomous Communities by the Ministry of Health, Social Services and Equality and the Health Information Institute.
Germany	*Data Protection Act 2018* (*Bundesdatenschutzgesetz*), repealing the 1990, 2009 and 2010 Acts; *E-Health Act 2015* (*Bundesministerium für Gesundheit*), amending *Social Code* (*Sozialgesetzbuch*), Book V.	
New Zealand	*Health Act 1956* (NZ) 1956/65; *Human Rights Act 1993* (NZ) 1993/82; *Privacy Act 1993* (NZ) 1993/28; and *Health Information Privacy Code 1994* (NZ).	New Zealand Interoperability Reference Architecture; and National Health IT Plan.
Switzerland	*Federal Act on Data Protection 1992* (*Bundesgesetz über den Datenschutz*); *Ordinance to the Federal Act on Data Protection 1993* (*Verodnung zum Bundesgesetz über Datenschutz*); and *Federal Act on The Electronic Patient File 2017* (*Gesetzbung Elektronisches Patientdossier*).	

Note: Cantons have individual laws on healthcare regulations.

III. Analysis

A. *Personal Access to Data by Individuals*

In all jurisdictions we studied, legislation and regulations provide patients with the right to access their own data. However, it is important to divide these systems to determine what patients have a right to access. Estonia introduced the Estonian National Health Information System ("ENHIS"), which provides a comprehensive overview of all patient information as part of a national health service ("NHS").[35] Registered healthcare providers (including natural or legal persons) must offer or forward the information to patients.[36] The patient has the right to access information and personal data concerning them using a web portal and a national ID card that stores their information.[37] The Australian MyHealth Record system is an opt-out national summary care record system.[38] These summary care records are made available to patients via a web portal linked to other social security and patient information.[39] The Italian system is based on health departments in different autonomous regions cooperating. However, the National Ministry of Health and the Data Protection Agency set standards for access to the NEHR system, the *Fascicolo sanitario electronico* ("FSE"). The Italian legislation simply requires the relevant local health authorities to make EHRs available to citizens online.[40] The Italian Data Protection Authority and Ministry of Health have also established the relevant guidelines for platform interoperability requirements.[41] This interoperability requires local health authorities to make a broad range of health services available, including booking, telemedicine, e-prescription and e-certificates.[42]

A similar federated system can be observed in Denmark and Spain.[43] In Denmark, a government-owned corporation MedCom manages the national summary care

---

35 *Health Services Organisation Act 2001* (Estonia), §59[1](3); *Statute of the Health Information System 2016* (Estonia) [*Estonia Health Information Statute*], Chapter 6, §22 [*Estonia Health Information Statute*]; Anna Essén *et al*, "Patient access to electronic health records: Differences across ten countries" (2018) 7:1 Health Policy and Technology 44 at 48.

36 *Estonia Health Information Statute, ibid*, Chapter 2, §5; OECD, *supra* note 19 at 63.

37 *Health Services Organisation Act 2014* (Estonia), Chapter 5[1], §59[3] [*Estonian Health Services Organisation Act 2014*]; *Estonia Health Information Statute, ibid*, Chapter 1, §4(4) and Chapter 5, §15, 16; *Personal Data Protection Act 2018* (Estonia), Chapter 4, Division 3, §22.

38 Garrety *et al*, *supra* note 6 at 6.

39 *MyHealth Records Act 2012* (Cth), s 15(a)(i) [*MyHealth Records Act 2012*].

40 *Decree Law No 221* (17 December 2012, Italy), Article 12, *Decree Law No 179* (18 October 2012, Italy), Article 12 [*Decree Law No 179*].

41 Italian Data Protection Authority, Guidelines on the Electronic Health Record and the Health File, (Italy: Italian Data Protection Authority July 2009), online: <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1672821>; Ministry of Health Italy, National eHealth Information Strategy, (Italy: Ministry of Health Italy, November 2011), online: Ministry of Health Italy <http://www.salute.gov.it/imgs/C_17_pubblicazioni_1653_allegato.pdf>.

42 *Ibid*.

43 For Denmark, see: *Health Act* (No 546 of 24 June 2005, Denmark), art 40; For Spain, see: *Patient Rights Act* (Law 41/2002, Spain), art 15 [*Spanish Patient Rights Act*]; the *National Health Service Quality Act* (Law 16/2003 of 28 May, Spain), art 54; Royal Decree 1093/2010 which Approves The Minimum Data Set Of Clinical Reports In The National Health System (Spain), Annex VIII; Royal Decree Law 7/2018 of 27 July on Universal Access to the National Health System (Spain), §157.

record system, Sundhed.dk.[44] This system collects data from each of the healthcare providers in the administrative regions of Denmark. Through the Sundhed.dk system, patients can access hospital EHRs, drug treatment records and patient appointments. All Danish residents are entitled to access healthcare services and can therefore access their national summary care record.[45] These EHRs can be accessed via the unique national identifier made available to Danish citizens.[46] Nevertheless, this right of access can be limited if it would conflict with public health matters or if their data is processed purely for scientific reasons.[47] In Spain, the *General Health Act* creates universal healthcare, but each autonomous community in Spain provides its own EHR design.[48] Each of these designs must be interoperable with a central node that manages communications and meet minimum security standards imposed by national law.[49] Further, the right of access to EHRs is guaranteed by both data protection law and patient rights legislation.[50] By contrast, the Singaporean NEHR is a government-owned platform operated by both the Ministry of Health and the Integrated Health Information Systems (IHiS). This system was designed to operate alongside the existing EHR systems that were used by physicians and hospitals.[51] Although there is not an explicit right to access data contained within the NEHR system, the Singaporean *Personal Data Protection Act* creates a right for data access broadly. However, this right is curtailed where there is a risk of harm to the patient requesting the data or others resulting from access.[52] Whilst the Singaporean government passed the *Healthcare Services Bill 2019* that protects patient rights,[53] this legislation does not apply to the NEHR. Instead, once security issues have been resolved, the question of NEHR rights will be addressed in subsequent revisions of the Act.[54]

In Germany, patients can access their EHRs via an e-Health card. Although the e-Health card was introduced following reforms in 2003,[55] further reforms in 2015

---

44 National Board of Health, *National Strategy for IT in the Hospital Sector 2003-7*, online: Danish Ministry of Health <https://www.sst.dk/~/media/5758F5105F0C400FB9CDC0D01D0F99EB.ashx>.

45 *Health Act* (Consolidated Act No 191 of 28 February 2018 on Health) (Denmark) at §7, 36-39 [*Denmark Health Act 2018*]; Patrick Kierkegaard, "eHealth in Denmark: A Case Study" (2013) 37:6 Journal of Medical Systems 9991 at 9992.

46 Denis Protti, Ib Johanesen & Francisco Perez-Torres, "Comparing the application of Health Information Technology in primary care in Denmark and Andalucía, Spain" (2009) 78:4 International Journal of Medical Informatics 270 at 276.

47 *Data Protection Act 2018* (No 502 of 23 May 2018, Denmark), §22(2), §22(5) [*Denmark Data Protection Act 2018*].

48 Isabel de la Torre-Díez, Sandra González & Miguel López-Coronado, "EHR Systems in the Spanish Public Health National System: The Lack of Interoperability Between Primary and Speciality Care" (2013) 37:1 Journal of Medical Systems 9914 at 9916.

49 *General Public Health Act* (Law 33/2011 of 4 October, Spain), arts 40-43; OECD, *supra* note 19 at 67.

50 *Spanish Patient Rights Act*, *supra* note 43, arts 4-6; *Protection of Personal Data and the Guarantee of Digital Rights Act* (Spain), art 13.

51 Ela Klecun *et al*, "The dynamics of institutional pressures and stakeholder behavior in national electronic health record implementations: a tale of two countries" (2019) 34(4) J Inf Technol 292 at 313.

52 *Personal Data Protection Act 2012* (No 26 of 2012, Sing), s 21(3)(a)-(b) [*Singapore PDPA 2012*].

53 *Healthcare Services Bill 2019* (Bill No 37/2019, Sing), s 57 [*Singapore Healthcare Services Bill*]. At the time of writing, this bill was scheduled to come into force in 2020.

54 *Parliamentary Debates Singapore: Official Report*, vol 94 at cols 51-53 (6 January 2020) (Mr Edwin Tong).

55 Eva Deutsch, Georg Duftschmid & Wolfgang Dorda, "Critical areas of national electronic health record programs—is our focus correct" (2010) 79(3) International Journal of Medical Informatics 211 at 215.

made this e-Health card mandatory for all citizens. Citizens were also provided with access to an interoperable summary care record online,[56] reinforced more generally by the 2018 reforms to German data protection law. Further, after the reforms the e-Health card doubles as a summary care record, containing the core data of the insured person, such as their address and date of birth.[57] Additional details will be added to the card in coming years, such as medication details.[58] Likewise, Swiss cantonal legislation mandates that health insurers provide electronic healthcare cards to insured patients that contain details on allergies and medications.[59] In 2013 the Swiss Federal Council (*Bundesrat*) also passed legislation mandating cantonal health agencies establish interoperable EHR systems. This legislation created an explicit right for patients to access their own data.[60] In a similar fashion to Denmark and Spain, healthcare providers in New Zealand have adopted what Coiera describes as a "middle-out" approach to implementing their NEHR.[61] This approach involves adopting national standards that healthcare providers must comply with, rather than a single system implemented nationally. Specifically, the New Zealand government offers a mechanism called "Health Internet" to allow different healthcare providers to communicate with one another.[62] Although there is no legislation to support these systems per se, patients can exercise their right under general privacy legislation to access EHRs from both public and private organisations.[63]

B. *Access Control for Data*

The requirement for access control raises the question of what uses of their data patients can consent to, as well as who can use it. In this context, a potential divide emerges between many of the European jurisdictions within our study relative to Australia, New Zealand and Singapore. This divide is partially attributable to European data protection law, which prohibits the processing of sensitive personal data (including health data) without explicit consent.[64] However, with the exception of Estonia and Spain, all of our European jurisdictions under consideration require explicit consent from patients to access EHRs for treatment. In the ENHIS, all registered healthcare professionals can access the EHRs for patients they are responsible for treating for healthcare purposes.[65] Nevertheless, patients have the right to block

---

56 *Social Code* (*Sozialgesetzbuch*), Book V, §15; §291 [*SGB*, Book V].

57 *Ibid*, §291(2).

58 Walter Gall *et al*, "The national e-medication approaches in Germany, Switzerland and Austria: A structured comparison" 93 International Journal of Medical Informatics 14 at 16 [Gall *et al*].

59 *Ibid* at 18.

60 *Federal Act on the Electronic Patient File 2017* (*Gesetzbung Elektronisches Patientdossier*) (Switzerland), art 8.

61 Coiera, *supra* note 19 at 272.

62 Denis Protti, Tom Bowden & Ib Johansen, "Adoption of information technology in primary care physician offices in New Zealand and Denmark, part 2: historical comparisons" (2008) 16:3 Journal of Innovation in Health Informatics 189 at 190.

63 *Health Information Privacy Code 1994* (NZ), clause 5, r 6 [*New Zealand Health Information Privacy Code 1994*].

64 *GDPR*, *supra* note 23, Recital 32.

65 *Estonian Health Services Organisation Act 2014*, *supra* note 37, Chapter 1, §3(1), §4^1(1), Chapter 5, §59^3.

access to certain health professionals for certain or all documents.[66] Further, patients can limit a healthcare provider's access to EHRs created as part of a healthcare service provision agreement.[67] The requirements are again different for access by third parties (such as employers, insurance companies and law enforcement agencies), with Danish law requiring explicit consent for access.[68] Spanish legislation does not explicitly exclude these third parties from access with consent, but Estonian, German and Italian legislation prohibits access to EHRs by these entities.[69] Finally, each of these jurisdictions creates certain rules on how EHR data can be accessed for research purposes. Denmark, Estonia and Italy have the most liberal regulations on research, with an opt-out research regime for non-identifiable data respectively with appropriate ethics approval.[70] By contrast, German and Spanish legislation require explicit consent for the reuse of patient data for research, except if the outcomes of research outweigh the rights of the patient.[71]

On the other hand, the original summary care record legislation in Australia required patient consent to the creation of their personally controlled summary care record.[72] However, amendments to the Act in 2015 introduced an opt-out consent model.[73] This reform was introduced on the belief this would improve the rates at which healthcare providers and patients participate.[74] Due to public outrage, an additional amendment extended the period from which patients could opt out from three to twelve months.[75] Nevertheless, patients cannot opt out of a healthcare identifier being created, which underpins the MyHealth Record system and collects documents from multiple repositories together.[76] Further, patients can object to certain documents being uploaded, but there is no requirement for healthcare providers to obtain consent before uploading a document.[77] Moreover, the System Operator can disclose information without the patient's consent to provide indemnity cover for a healthcare provider, or where ordered by a court or tribunal.[78] Likewise, the Singaporean legislative regime also provides a significant scope to release information for both

---

66 *Estonia Health Information Statute, supra* note 35, Chapter 5, §19(1)-(2), *Health Services Organisation Act 2018*, Chapter 5, §59^3(3)-(4).

67 *Estonia Health Information Statute*, *ibid*, Chapter 5, §19(3)

68 *Denmark Health Act 2018*, *supra* note 45, §43-44, 46-48; *Denmark Data Protection Act 2018*, *supra* note 47, §10.

69 *Denmark Data Protection Act 2018*, *ibid*, §10(1) (Processing of personal data in connection with violation of obligation); *SGB*, Book V, *supra* note 56, §15; §291a(8); *Decree Law No 179*, *supra* note 40, arts 12(2)-(4); Italian Data Protection Agency, supra *note* 39 at 6-8.

70 *Denmark Health Act 2018*, *supra* note 45, §43-44, 46-48; *Denmark Data Protection Act 2018*, *supra* note 47, §10; Health Services Organisation Act 2018, Chapter 5, §59^4 (1), (3); *Decree Law No 179*, *ibid*, arts 12(2), 12(6).

71 *Spanish Patient Rights Act*, *supra* note 43, art 16; *Protection of Personal Data and the Guarantee of Digital Rights Act* (Law 3/2018 of 6 December), Seventeenth Additional Provision 2(b).

72 *Personally Controlled Electronic Health Records 2012* (Cth), ss 39, 40.

73 *Health Legislation Amendment (eHealth) Act 2015* (Cth), Part 2.

74 Jillian Oderkirk, *Readiness of electronic health record systems to contribute to national health information and research*, OECD Health Working Papers No 99 (2017), online: OECD iLibrary <https://doi.org/10.1787/9e296bf3-en>, at 41.

75 *MyHealth Records Amendment (Strengthening Privacy) Bill 2018* (Cth)

76 *Healthcare Identifiers Act 2010* (Cth), s 9.

77 Gabrielle Wolf & Danuta Mendelson, "The My Health Record System: Potential to Undermine the Paradigm of Patient Confidentiality" (2019) 2 UNSWLJ 619 at 627 [Wolf & Mendelson].

78 *MyHealth Records Act 2012*, *supra* note 39, ss 68, 69, 69A, 70.

third-party purposes (such as quality assurance and insurance) and scientific research without consent.[79] Nevertheless, researchers must comply with data handling measures under the Human Biomedical Research Act for biomedical research,[80] as well as the Personal Data Protection Act provisions for research more broadly. An institutional review board also must decide whether general consent or a waiver of consent is appropriate for the project.[81] In New Zealand, health information cannot be used or disclosed for any purpose other than for which they were originally collected. Further, in both New Zealand and Singapore, EHRs and patient data can only be used and disclosed for research where patients are not identifiable or could not be reasonably expected to be identified.[82] Finally, the general jurisprudence from New Zealand case law is that personal information will be defined broadly to depend on the context in which it is used.[83] Nevertheless, the Health Act still, controversially, makes certain sets of data available for research (such as for the National Cervical Screening Programme).[84]

C. *Right to Add and Correct Data*

The right to add and correct health data is equivalent to the right to add or correct incorrect or missing data under EU and European data protection law.[85] However, this right was not available for NEHR data for all jurisdictions in our study. In Denmark and Germany, patients are expressly forbidden from correcting data themselves in their own EHR and must instead request correction under data protection law. The only exception to this prohibition is over-the-counter medication under Danish law. Although not expressly forbidden under Spanish law, in practice only physicians can add or correct a patient's EHR data. Likewise, under New Zealand and Singaporean law, patients cannot explicitly modify their own data and must rely on data protection law to request that it be modified.[86] However, in Estonia and Switzerland patients can make "declarations of intent" in their EHR, indicating how they want their personal data, tissue or organs to be used post mortem.[87] These declarations of intent sit alongside the right to request that incorrect data, including health data, be erased.[88] In Italy, patients cannot correct data in the FSE, but have access to a personal notebook (in Italian: *taccuino*) in which patients can add their own notes

---

79 *Singapore PDPA 2012*, *supra* note 52, s 17(1), Second Schedule; *Singapore Healthcare Services Bill*, *supra* note 53, ss 51(2)-(4).

80 *Human Biomedical Research Act 2015* (No 29 of 2015, Sing), ss 27(3), 28 [*Singapore Human Biomedical Research Act 2015*]; *Singapore PDPA 2012*, *ibid*, Third Schedule, paras 1(i), 2.

81 *Singapore Human Biomedical Research Act 2015*, *ibid*, ss 12, 14.

82 *New Zealand Health Information Privacy Code 1994*, *supra* note 63, clause 5, rs 10-11; *ibid*, s 3.

83 Joshua Yuvaraj, "How about me? The scope of personal information under the Australian *Privacy Act 1988*" (2018) 34(1) Computer Law & Security Review 47 at 56.

84 *Health Act 1956* (NZ) 1956/65, Part 4A; Katherine Wallis, "Cervical screening legislation is unethical and has the potential to be counterproductive" (2007) 120(1266) New Zealand Medical Journal 69 at 70.

85 *GDPR*, *supra* note 23, art 15.

86 *New Zealand Health Information Privacy Code 1994*, *supra* note 63, clause 5, r 7; *Singapore PDPA 2012*, *supra* note 52, s 22.

87 *Estonia Health Information Statute, supra* note 35, Chapter 5, §21; Federal law on the electronic patient file (EPDG) 15 June 2017, art 8.

88 *Federal Act on Data Protection* (*Bundesgesetz über den Datenschutz*) 1992, art 5(1).

regarding their health.[89] We discuss the legal and ethical implications of Italian patients have control over their own personal notebook in the fourth section of this paper. Similarly, the Australian regulations provide patients with an equivalent right to add data to their own records. These include declarations of intent, medication summaries and advanced healthcare planning information.[90]

D. *Right to Erase Data*

The availability of the right to erase data from EHRs is perhaps the most inconsistent across the nine jurisdictions we examined. Specifically, only four (Australia, Denmark, Estonia and Italy) permit data subjects to delete their data.[91] Further, the availability of the right is restricted in these jurisdictions. In Denmark and Estonia patients can delete data submitted as part of a declaration of intent or on self-prescribed medicine.[92] Nevertheless, in these jurisdictions, patients cannot request that data uploaded by a healthcare provider be deleted. Whilst Estonian and Danish data protection law recognises a general right of erasure, it is uncertain whether this right extends to include EHRs. Recent EHR standards suggest erasure is not a universal function.[93] In Italy, patients also cannot change the information uploaded into their EHRs by doctors. However, patients still have complete control over data they enter into their personal notebooks.[94] Australia offers a significant degree of control to patients over the erasure of their data stored in the MyHealth Record system. Initially, the Australian government adopted an opt-in consent approach for the MyHealth Record system, under which patients could request to cancel their account. However, this cancellation right did not guarantee patients their data would be subsequently erased from any database.[95] Instead, patient data would be archived for 30 years after death.[96] After public outcry,[97] the legislation was amended to include a requirement that data be erased. Further, the MyHealth Record legislation provides patients with the capacity to prevent practitioners from viewing documents.[98] The effect of this removal is that practitioners may be unaware of the fact that the document existed in the first place.[99]

---

89 *Decree Law No 179*, *supra* note 40, arts 12(3), 13(2).

90 *MyHealth Records Rules* 2016 (Cth), r 4(2) ('advanced healthcare planning information', 'healthcare recipient-entered health summary'), r 6(2).

91 *Estonia Health Information Statute, supra* note 35, §17(2).

92 Executive Order of the Danish Medicines Agency's electronic registration of individual citizens' medical information 2011, art 25, online: Global Regulation <https://www.global-regulation.com/translation/denmark/611809/executive-order-on-the-danish-medicines-agencys-electronic-registration-of-individual-citizens–medication-information.html>.

93 Duarte Gonçalves-Ferreira *et al*, "OpenEHR and General Data Protection Regulation: Evaluation of Principles and Requirements" (2019) 7:1 JMIR Medical Informatics e9845 at 9.

94 *Decree Law No 179*, *supra* note 40, arts 12(3), 13(2).

95 Mendelson, *supra* note 23 at 27.

96 *MyHealth Records Act 2012*, *supra* note 39, s 17 (incorporating Health Legislation Amendment (eHealth) Act 2015.

97 Robert Merkel, *My Health Record: Deleting personal information from databases is harder than it sounds* (2 August 2018), online: The Conversation <https://theconversation.com/my-health-record-deleting-personal-information-from-databases-is-harder-than-it-sounds-100962>.

98 *MyHealth Records Rules 2016* (Cth), rs 5(e), 6(1).

99 Australian Digital Health Agency, *How to remove information*, online: Australian Digital Health Agency <https://www.myhealthrecord.gov.au/for-you-your-family/howtos/remove-information>.

IV. Discussion

We will now examine the points of convergence and divergence in each jurisdiction.

A. *Areas of Convergence*

The first area of convergence that we identified in each jurisdiction was the right of access. Irrespective of whether there is a patient accessible NEHR or whether patients must request access, all patients are entitled to access their data. Increasingly, whether via policy or legislation, jurisdictions are allowing patients to access their EHRs via an electronic portal or an electronic health card.[100] This convergence appears to be an apotheosis of a technical and policy perspective that patient accessible EHRs encourage patient empowerment and reinforce trust between patients and physicians.[101] The second area of convergence relates to patient control over the physicians who can access their EHRs. Specifically, all the jurisdictions that we studied allowed patients to place limits on the physicians who could access their EHRs for care purposes. This finding reflects patient attitudes towards sharing health information, who preferred to be consulted first.[102] Nevertheless, as the next section discusses, we did not identify the same degree of convergence with respect to access control by other parties.

B. *Areas of Divergence*

The first noticeable area of divergence concerns which third parties can access patient data from EHRs. Whilst the European jurisdictions and New Zealand require explicit patient consent for third parties to access EHRs, both Australia and Singapore permit some forms of access without consent. As Wolf and Mendelson note regarding the MyHealth Record system, permitting access without consent has severely damaged patient trust, precipitating high opt-out rates. Further, once this trust is lost, it may be difficult for governments to regain it.[103] Although Singapore shares Australia's "light touch" privacy legislative regime,[104] establishing the boundaries of a governance model will be key to the success of the nascent Singaporean NEHR system.[105] The second area of divergence is with respect to how data may be used for research purposes, in which we identify three approaches. The first approach explicitly requires

---

[100] Bradford Gray *et al*, "Electronic health records: an international perspective on "meaningful use"" (2011) 28 Commonwealth Fund Issue Briefs 1 at 5.

[101] Meredith Carter, "Should patients have access to their medical records?" (1998) 169:11-12 Medical Journal of Australia 596 at 597; Christian Nøhr *et al*, "Nationwide citizen access to their health data: analysing and comparing experiences in Denmark, Estonia and Australia" (2017) 17:1 BMC Health Services Research 534 at 543.

[102] Richard Whiddett *et al*, "Patients' attitudes towards sharing their health information" (2006) 75:7 International Journal of Medical Informatics 530 at 537.

[103] Wolf & Mendelson, *supra* note 77 at 651.

[104] Warren B Chik, "The Singapore Personal Data Protection Act and an assessment of future trends in data privacy reform" (2013) 29 Computer Law & Security Review 554 at 558.

[105] Susan Ee Ong *et al*, "Health system reforms in Singapore: A qualitative study of key stakeholders" (2018) 122:4 Health Policy 431 at 438.

Table 2. Rights available in examined jurisdictions.

	Right			
	Personal Access	**Access Control**	**Add/Modify Data**	**Delete/Erase Data**
Australia	Yes, electronically	Yes (Physicians) Partial (Third Parties)	Yes (Contact Details, Declarations of Intent, Medication, Care Plans), Personal Control	Yes
Denmark	Yes, electronically	Yes (Physicians, Third Parties) Partial (Researchers*)	Partial (Contact Details, Declarations of Intent, Medication), Personal Control	Partial (Contact Details, Declarations of Intent, Medication)
Estonia	Yes, electronically	Yes (Physicians, Third Parties) Partial (Researchers*)	Partial (Contact Details, Declarations of Intent, Medication), Personal Control	Partial (Contact Details, Declarations of Intent, Medication)
Germany	Yes, electronically and by request	Yes (Physicians, Third Parties, Researchers)	No, Only by Request	No
Italy	Yes, electronically and by request	Yes (Physicians, Third Parties) Partial (Researchers*)	Yes (Contact Details, Declarations of Intent, Medication, Care Plans), Personal Control	Yes
New Zealand	Yes, electronically and by request	Yes (Physicians, Third Parties) Partial (Researchers*)	No, Only by Request	No
Singapore	Yes, by request	Yes (Physicians) Partial (Third Parties)	No, Only by Request	No
Spain	Yes, electronically	Yes (Physicians, Third Parties, Researchers)	No, Only by Request	No
Switzerland	Yes, electronically or request	Yes (Physicians, Third Parties) Partial (Researchers*)	Partial (Contact Details, Declarations of Intent, Medication), Personal Control.	Partial (Incorrect data only)

* Control extends to identifiable data only.

consent for data to be used for research purposes and is present in Germany and Spain. By contrast, the second approach involves permitting research on de-identified data without consent, but require consent for accessing identifiable data. Finally, jurisdictions such as Australia and Singapore permit access to identifiable data for public interest research. Identifiable data may also be accessible in EU jurisdictions where a public interest exists, such as for health research.[106] The latter two approaches recognise the public benefits that may flow from research using EHR data.[107] Nevertheless, the use of data for research requires balancing between protecting patient privacy and ensuring utility of data, given the difficulty of producing useful yet anonymised data. The fragmented definitions of what constitutes anonymised data represents a further point of divergence between our jurisdictions.[108] For example, Estonia is currently regarded as one of the most liberal nations with respect to the use of data for patient research. However, prior to this Estonian data protection law did not contain an exception for research as a secondary purpose without consent.[109] These limitations significantly undermined the usability of data collected for the Estonian Cancer Registry by preventing data linkage. This situation persisted until 2007, when legislative reforms created a specific exception to reuse data for scientific research without consent.[110]

The third and fourth areas of divergence was with respect to whether patients can just add or also correct and erase their data, as well as what types they could add or correct. Five out of the nine jurisdictions we examined allowed patients to upload information to their EHRs, whilst four of those five included a right of erasure. Of those four, two (Denmark and Estonia) granted patients the right to upload limited details such as personal details, gender and medication or vaccination details. In part, these data types are modifiable because these countries have chosen to focus on summary care records and e-prescribing as the first stage of implementing NEHRs.[111] Although ostensibly Australia and Italy have opted for summary care records, health departments in these countries have gone much further in offering patients control over the data in their EHR. Further, the consequences of the extended right of control may seriously disrupt existing practitioner-patient relationships. A potent example of this disruption is the right of erasure contained within the MyHealth

---

[106] Article 29 Data Protection Working Party, *Opinion on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC*, EC Opinion WP 217 (2014), online: European Commission <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf>, 21-23.

[107] Søren Holm & Thomas Ploug, "Big Data and Health Research—The Governance Challenges in a Mixed Data Economy" (2017) 14:4 Journal of Bioethical Inquiry 515 at 518.

[108] Danuta Mendelson & Gabrielle Wolf, "My [electronic] Health Record—cui bono (for whose benefit)?" (2016) 24:2 JLM 283 at 293 [Mendelson & Wolf].

[109] Mati Rahu & Martin McKee, "Effect of Estonian law on prospects for public health research" (2003) 362:9401 Lancet 2122.

[110] Mati Rahu & Martin McKee, "Epidemiological research labelled as a violation of privacy: the case of Estonia" (2008) 37:3 International Journal of Epidemiology 678 at 679-680; Kaire Innos, Aleksei Baburin & Tiiu Aareleid, "Cancer patient survival in Estonia 1995-2009: Time trends and data quality" (2014) 38:3 Cancer Epidemiology 253.

[111] Simon de Lusignan *et al*, "A Comparison of Approaches to Providing Patients Access to Summary Care Records Across Old and New Europe: An Exploration of Facilitators and Barriers to Implementation" (2013) 192 Studies in Health Technology and Informatics 397 at 398; Gall *et al*, *supra* note 58 at 18.

Record legislative framework. The fact that a patient can hide documents from a physician's view entirely may prevent healthcare organisations from guaranteeing continuity of care.[112] Likewise, the *taccuino* in the Italian NEHR raises several legal questions regarding the liability and responsibilities of patients and physicians. Beyond clinical continuity, these include who the data controller and processor are for a patient-controlled EHR, what role informed consent plays and who is liable for medical errors.[113] Whilst the *GDPR* creates scope for joint controllership and patients arguably "own" the data in their EHR,[114] the effect on responsibilities under data protection law remains uncertain. Further, there is an open question as to whether the information in a patient's private EHR should be made available for physicians to access for treatment.[115] The types of information that are accessible may change as specific databases (such as the Danish Vaccination registry) are incorporated into more comprehensive EHR systems.

C. *Towards a Tentative Typology of Patient Rights for NEHRs*

Having examined the differences between the nine jurisdictions above in a deductive-inductive fashion, we can now derive the main dimensions of patient rights for data stored in NEHRs. To do so, we will refer to the four principles of biomedical ethics for examining these dimensions. These four principles are respect for autonomy, non-maleficence, benefiting others and justice.[116] First, we note that there is a clear public/private dichotomy in patient rights. Although the public/private spectrum in privacy scholarship refers to a spatial concept,[117] we use it to describe potential uses for NEHRs. On one end of this spectrum, NEHRs provide patients with a greater degree of flexibility to transfer their EHR between healthcare providers, supporting autonomy. Patients can also include additional personal information about their treatment, tying to the broader socio-technical concept of the quantified self.[118] This control over the EHR itself, rather than the nature of treatment, reflects a tendency towards "multilateral" as opposed to "bilateral privacy".[119] On the other end, NEHRs provide useful data for public health research, government agencies and scientific research on population level data. However, the justifiability of using NEHRs for these purposes vary between the types of use in question. For example, research directed towards health system functioning or publicly funded research offers benefit to the general population at large and therefore represents a

---

112 Mendelson & Wolf, *supra* note 108 at 292.

113 Paolo Guarda & Rossana Ducato, "From electronic health records to personal health records: emerging legal issues in the Italian regulation of e-health" (2016) 30:3 International Review of Law, Computers & Technology 271 at 277 [Guarda & Ducato].

114 *GDPR*, *supra* note 23, art 26.

115 Guarda & Ducato, *supra* note 113 at 279.

116 Tom L Beauchamp & James F Childress, *Principles of Biomedical Ethics*, 7th ed (Oxford: Oxford University Press, 2013) at 57, 113, 165, 225, 312.

117 Koops *et al*, *supra* note 18 at 544-554.

118 Michele Loi *et al*, "Cybersecurity in health—disentangling value tensions" (2019) 17:2 Journal of Information, Communication and Ethics in Society 229 at 234.

119 Roger S Magnusson, "The Changing Legal and Conceptual Shape of Health Care Privacy" (2004) 32:4 J.L. Med. & Ethics 680.

significant public good.[120] By contrast, it may be more difficult to justify secondary research carried out by commercial entities as representing a public good. Most of the jurisdictions we examine attempt to resolve this conflict between autonomy and benefiting others by allowing patients to deny physicians access to certain documents with personal data.[121] In other cases (notably Australia), patient autonomy to make documents available overrides the potential benefit to others. Although ostensibly done to encourage patient ownership and partnership between patients and physicians, Mendelson and Wolf argue these stated goals of the MyHealth Record system disguise its consumer-oriented nature.[122]

The question of the public/private dichotomy dovetails neatly into the divide between different forms of data. This divide exists between different forms of health-related data, as well as who generates this data and whether it is identifying or not. In some cases, the legislation clearly establishes that patients have greater control over certain forms of data (such as contact details and testamentary intention). In the case of Australia and Italy, control over patient entered healthcare data receives priority over other principles (such as certain physicians having this data available for clinical treatment). However, in other cases, patients are increasingly limited with respect to the uses of data they can control. In all of the jurisdictions that we studied, patients do not have complete control over their de-identified data. Instead, regulations create space for researchers and government to access de-identified data without consent or identifying data where a public interest exists. Although there is an obvious case of benefiting others and justice to the broader population from permitting access, it comes at a potential cost to patient privacy.[123] Further, in Australia, New Zealand and Singapore, the dimension of data access in turn dovetails into which entities can access identifiable patient data. For example, permitting health insurance agencies, tribunals and law enforcement agencies to access patient EHRs without consent or other safeguards can compromise patient autonomy and beneficence. To ally public concerns,[124] the Singapore Healthcare Services Bill prevents the release of health information without consent unless a statute exists to govern reasonable requests to access that data.[125] The final divide that we identify is who bears ultimate responsibility for managing their EHRs. For the most part, patient autonomy here is subordinate to beneficence and non-maleficence; in other words, to guarantee quality of care, patients cannot modify their own data. However, as discussed above, Australia and Italy represent two outliers where patients can upload data to their EHRs, with the resultant impact of patent autonomy subordinating beneficence uncertain. We submit these shifts towards prioritising patient autonomy

---

120 Katharine A Wallis *et al*, "Research using electronic health records: Balancing confidentiality and public good" (2018) 10:4 Journal of Primary Health Care 288 at 290.

121 Eric M Meslin & Peter H Schwartz, "How Bioethics Principles Can Aid Design of Electronic Health Records to Accommodate Patient Granular Control" (2015) 30:1 Journal of General Internal Medicine 3 at 4.

122 Mendelson & Wolf, *supra* note 108 at 285.

123 Mark A Rothstein, "Is Deidentification Sufficient to Protect Health Privacy in Research?" (2010) 10:9 American Journal of Bioethics 3 at 8.

124 College of Family Physicians Singapore, Academy of Medicine Singapore & Singapore Medical Association, *Joint Survey on the Public Sentiments towards the National Electronic Health Record*, online: Singapore Medical Association <https://www.sma.org.sg/UploadedImg/files/Publications%20-%20SMA%20News/5008/Survey.pdf>.

125 *Singapore Healthcare Services Bill*, *supra* note 53, s 51(2).

can be exploited as part of a broader neoliberal approach to social welfare adopted by modern governments.[126] Nevertheless, imposing market logic onto NEHR systems blurs the boundaries between patient control (and implicit liability) and ownership over data, leading to patient mistrust and refusal to participate.[127]

V. Conclusion

Following our analysis, we argue that NEHR implementations should be neither considered patient property nor a means of outsourcing liability to patients. Instead, NEHRs should be conceived as a public good. No universal framework for success exists to guarantee the sustainability of public goods.[128] However, our comparative analysis suggests that patient rights are crucial to governing NEHRs as a public good. We submit that the impact of these patient rights on NEHRs should be considered according to the dimensions of our typology. This typology includes the actors who can access data, the types of data and the purposes for which data are used. Determining the appropriate extent of each patient's right is therefore dependent on the competing bioethical principles embodied in each context. For example, the public backlash in Singapore against broad access to NEHR data demonstrates the risks of prioritising beneficence over autonomy. Further, the legislation in Singapore and Australia shows undue encroachment by beneficence on patient autonomy is not necessarily confined to countries without specific NEHR legislation.

Instead, we submit regulations or legislation governing NEHRs should delineate the rights and responsibilities of physicians, patients and third parties. For example, if patients have the right to enter and erase their own data, the consequences of this decision for quality of care and liability should be identified. Likewise, whether identifiable or anonymised patient data is available for primary or secondary research should be identified. Finally, we submit that for distinguishing between different forms of technology supporting patient rights (namely, deidentification and patient access), legislation should remain technology agnostic. Instead, regulations that can be modified adaptively should be used to set the necessary protocols and technical requirements. For example, the majority of data collected from EHRs, including audit data, is not identifying.[129] Nevertheless, regulations should be capable of reacting to novel technological avenues of indirect reidentification. Likewise, in the case of the previous Estonian data protection regime, the regulatory framework lacked sufficient flexibility to allow researchers to link data for epidemiological research purposes. Therefore, technical mechanisms (such as granular consent controls) should be installed in personally accessible NEHR portals. These will provide patients with greater ability to control the uses of their data.

---

[126] Susan Baines, Penelope Hill & Karin Garrety, "What Happens When Digital Information Systems Are Brought Into Health and Social Care? Comparing Approaches to Social Policy in England and Australia" (2014) 13:4 Social Policy & Society 569 at 575.

[127] Paraskevas Vezyridis & Stephen Timmons, "On the adoption of personal health records: some problematic issues for patient empowerment" (2015) 17:2 Ethics and Information Technology 113 at 117.

[128] Thomas Dietz, Elinor Ostrom & Paul C Stern, "The Struggle to Govern the Commons" (2003) 302:5652 Science 1907 at 1912.

[129] Mann, Savulescu & Sahakian, *supra* note 16 at 15.