Can Distributed Ledger Technology Support Auditability of Patient Data in Electronic Health Records? A Comparative Legal Study

JAMES SCHEIBNER[*], MARCELLO IENCA[**], AND EFFY VAYENA[***]

Abstract

After both national governments and healthcare institutions have attempted moving towards using electronic health records ('EHRs'), access control, transparency, and auditability have emerged as important success factors. Distributed ledger technology ('DLT') has been proposed as a mechanism to allow patients to control their electronic health records. Underpinning 'smart contracts', DLT might help automate and streamline the consent and healthcare management process. However, the degree to which DLT can remain compatible with auditability requirements imposed by current data privacy regulations remains an ongoing implementation challenge. In this paper, we present a comparison of auditability requirements for EHRs in five jurisdictions: United States, Australia, Switzerland, the European Union, and the Council of Europe. Further, we examine the extent to which DLT can help satisfy these auditability requirements. Following our comparative doctrinal analysis, we identify similarities but conclude there is no universal granular definition for auditability in the five jurisdictions we examine. Therefore, we argue that DLT and smart contracts cannot oust the role of legal regulation with respect to patient data. Nevertheless, in concert with regulation, further encryption mechanisms, and patient education, this technology can provide a mechanism to satisfy the need for patients, physicians, and researchers to access auditable EHRs. We then use these three case studies to demonstrate the potential of DLT in an ethically and legally integrated implementation approach.

1 Introduction

Electronic Health Records ('EHRs') can introduce three benefits for improving personalised healthcare and public health management. First, patients who can access their own EHRs may have an increased feeling of control and

[*] Lecturer, College of Business, Government and Law, Flinders University, Adelaide, Australia.

[**] Principal Investigator, College of Humanities, EPFL Lausanne, Lausanne, Switzerland.

[***] Chair of Bioethics, Health Ethics and Policy Laboratory, Department of Health Sciences and Technology, ETH Zürich, Switzerland. Corresponding Author. All post publication inquiries should be directed to effy.vayena@hest.ethz.ch. This paper was written as part of the Data Protection in Personalised Health Project ('DPPH'). This project was supported by the grant #2017-201 of the Strategic Focal Area 'Personalized Health and Related Technologies ('PHRT')' of the ETH Domain.

responsibility over their healthcare.[1] Secondly, physicians and healthcare institutions can use EHRs to provide superior continuity and quality of care.[2] Thirdly, medical researchers can perform superior public health and scientific research with access to patient data stored in EHRs.[3] Surveys suggest that patients support these secondary uses, provided that the benefits are adequately balanced against any perceived risks such as unauthorised disclosure of data.[4] Without safeguards to protect against these risks, patients and physicians may attempt to opt out of participating in the secondary use of data from EHR systems. Consequently, the benefits from collective participation will be lost.[5]

One case study demonstrating this phenomenon is the *care.data* programme in the United Kingdom. This programme was developed to make UK National Health Service ('NHS') health records available for public health and research use in a data registry. However, after NHS Digital only gave patients and doctors eight weeks' notice to opt out of the register, *care.data* suffered an enormous public backlash .[6] Likewise, the My Health Record system in Australia is designed to make summary care data available for research and public health purposes. However, the Australian legislative framework has already undergone significant revision due to public concerns about controlling who has access to the records.[7] Finally, French patients and physicians have baulked at opting into

[1] Eva Deutsch et al, 'Critical Areas of National Electronic Health Record Programs — Is Our Focus Correct?' (2010) 79(3) *International Journal of Medical Informatics* 211, 215, 217.

[2] Carlo De Pietro and Igor Francetic, 'E-Health in Switzerland: The Laborious Adoption of the Federal Law on Electronic Health Records (HER) And Health Information Exchange (Hie) Networks ' (2018) 122(2) *Health Policy* 69, 73.

[3] Mhairi Aitken, Sarah Cunningham-Burley and Claudia Pagliari, 'Moving from Trust to Trustworthiness: Experiences of Public Engagement in the Scottish Health Informatics Programme' (2016) 43(5) *Science and Public Policy* 713, 713–714.

[4] Fiona Riordan et al, 'Patient and Public Attitudes towards Informed Consent Models and Levels of Awareness of Electronic Health Records in the UK' (2015) 84(4) *International Journal of Medical Informatics* 237, 238, 245–6.

[5] James Scheibner et al, 'Benefits, Challenges, and Contributors to Success for National EHealth Systems Implementation: A Scoping Review' (2021) 28(9) *Journal of the American Medical Informatics Association* 2039, 2044.

[6] Sigrid Sterckx et al, '"You Hoped We Would Sleep Walk into Accepting the Collection of Our Data": Controversies Surrounding the UK Care.Data Scheme and Their Wider Relevance for Biomedical Research' (2016) 19(2) *Medicine, Health Care and Philosophy* 177, 181–8; Miranda Mourby et al, 'Health Data Linkage for Public Interest Research in the UK: Key Obstacles and Solutions' (2019) 4(1) *International Journal of Population Data Science*, 5.

[7] Gabrielle Wolf and Danuta Mendelson, 'The My Health Record System: Potential to Undermine the Paradigm of Patient Confidentiality' [2019] (2) *University of New South Wales Law Journal* 619, 650; Deborah Lupton, '"I'd like to Think You Could Trust the Government, but I Don't Really Think We Can": Australian Women's Attitudes to and Experiences of My Health Record' (2019) 5 *Digital Health* 2055207619847017.

the Dossier Médical Personnel due to ongoing technical issues and the government's poor explanation of the system's benefits.[8]

On the one hand, these case studies paint a dire picture of the future of electronic health record systems. On the other hand, patients still support the use and storage of their data in EHR systems in systematic reviews, surveys, and empirical studies, including those referenced previously.[9] Patient observations in these studies suggest that patients are not opposed to EHRs, but instead want mechanisms that allow them to audit and control the use of their data. Computer scientists and medical researchers have therefore proposed several technological solutions to increase the auditability of electronic patient records.

One of these solutions is distributed ledger technology ('DLT'), which involves using a cryptographic algorithm to verify the record integrity of a distributed network or ledger.[10] Further, all transactions or transfers of data are distributed across multiple nodes, so that information about data transactions or transfers cannot be modified without group consensus. Although associated with the 'trustless transaction' mechanism of cryptocurrencies such as *Bitcoin*, policy scholars classify DLT as a general-purpose technology capable of aiding governance in other domains.[11] One of these is as a mechanism for custodians of EHR systems to track and share patient data.

A technical concept related to DLT is a 'smart contract' — a self-executing and autonomous digital transaction underpinned by cryptographic algorithms.[12] Although, conceptually, smart contracts can exist without DLT, numerous DLT implementations underpin 'smart contracts' that promise to automate EHR

[8] Brigitte Séroussi and Jacques Bouaud, 'Adoption of a Nationwide Shared Medical Record in France: Lessons Learnt after 5 Years of Deployment' (2017) *2016 AMIA Annual Symposium Proceedings* 1100.

[9] Riordan et al (n 4) 240; Sterckx et al (n 6), 182. See also Alexander Hoerbst et al, 'Attitudes and Behaviors Related to the Introduction of Electronic Health Records among Austrian and German Citizens' (2010) 79(2) *International Journal of Medical Informatics* 81, 87; Jessica Stockdale, Jackie Cassell and Elizabeth Ford, '"Giving Something Back": A Systematic Review and Ethical Enquiry into Public views on the Use of Patient Data for Research in the United Kingdom and the Republic of Ireland' (2019) 3 *Wellcome Open Research* 6, 14–15; Richard Whiddett et al, 'Patients' Attitudes Towards Sharing their Health Information' (2006) 75(7) *International Journal of Medical Informatics* 530, 537.

[10] Michèle Finck, 'Blockchains: Regulating the Unknown' (2018) 19(4) *German Law Journal* 665, 667.

[11] Svein Ølnes, Jolien Ubacht and Marijn Janssen, 'Blockchain in Government: Benefits and Implications of Distributed Ledger Technology for Information Sharing' (2017) 34(3) *Government Information Quarterly* 355, 355–6.

[12] Kevin Werbach and Nicolas Cornell, 'Contracts Ex Machina' (2017) 67(2) *Duke Law Journal* 313, 317; Konstantinos Christidis and Michael Devetsikiotis, 'Blockchain and Smart Contracts for the Internet of Things' (2016) 4 *IEEE Access* 2292, 2296.

management.[13] Early technical and legal literature on smart contracts have gone further than such modest claims, and have advocated for replacing courts with technical mechanisms.[14] Nevertheless, any custodian of EHRs is still required under data protection and privacy law to ensure the confidentiality and security of these records. Accordingly, the question of legal compliance and DLT is recursive. That is, how can DLT help ensure compliance while simultaneously remaining compliant with data protection law?

Therefore, this paper assesses how DLT can be used to support auditability requirements under data protection law for patient data stored in EHRs. In turn, our assessment can be used to inform architecture design and technical requirements for DLTs in healthcare. To achieve this goal, we contextually examine DLT in light of the international data protection landscape. Specifically, we compare how auditability has been defined with respect to electronic health data in five jurisdictions and explore the extent to which DLT can enable EHR auditability. Our paper is split into two sections. Our first section provides a comparison of auditability requirements under relevant legislation and regulations in the United States ('US'), Australia, the European Union ('EU'), Switzerland, and the Council of Europe. These jurisdictions were purposively selected because they exemplify a range between comparatively weak and strong data protection legislation. Accordingly, this section examines these jurisdictions in the order of their granularity and level of auditability requirements (United States, Australia, EU, Switzerland and Council of Europe). This comparison is necessary to determine which requirements are imposed by legislation onto the processors and controllers of EHRs, and which are best practices. Our second section then considers the boundaries and limitations of DLT architecture with respect to managing EHRs. It concludes by discussing how DLT might support legally compliant auditability for EHRs in three case studies of use by different stakeholders: patients in accessing and controlling their records, physicians in using the records to provide continuity of care, and researchers in using the information for research purposes.

2 *Technical and Legal Concepts of Auditability Regarding EHRs*

2.1 Technical Concepts of Auditability

Before addressing how different jurisdictions support the auditability of EHRs, it is first necessary to define auditability and explain its conceptual relevance to EHRs. Because of the sensitive nature of healthcare records, one of the greatest

[13] Gary Leeming, James Cunningham and John Ainsworth, 'A Ledger of Me: Personalizing Healthcare Using Blockchain Technology' (2019) 6 *Frontiers in Medicine* <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6668357/>.

[14] For a critique of these challenges, see Alexander Savelyev, 'Contract Law 2.0: "Smart" Contracts and the Beginning of the End of Classic Contract Law' (2017) 26(2) *Information & Communications Technology Law* 116, 128.

challenges with respect to implementing EHRs is ensuring adequate security measures exist. It is important to ensure that access control mechanisms are in place to ensure that access is limited to authorised users.[15] These access control mechanisms should only permit users to use or modify patient data that they have permission to access. This is particularly important where records are shared between healthcare organisations, so that only users (such as healthcare practitioners) can view records sent to them.[16]

Further, access control mechanisms should allow a system administrator to view which users have accessed a particular record, and whether they had permission to do so.[17] This functionality, which we will refer to as 'auditability' in this article, is therefore a fundamental security requirement for EHRs. We will now turn to address how privacy legislation and regulations that apply to EHRs in different jurisdictions attempt to support this auditability requirement.

2.2 United States

The *Health Insurance Accountability and Accessibility Act* ('HIPAA') and the associated *Security Rule* impose technical requirements for electronic protected health information held by covered entities.[18] These include healthcare and health insurance providers, as well as health clearing houses.[19] 'Protected health information' includes any health information that identifies or could reasonably identify an individual.[20] In addition, the business associates of covered entities must also comply with these security requirements. Such business associates include those entities providing data transmission services, offering personal health records on behalf of a covered entity, or otherwise providing subcontracted services.[21] Further, there may be 'hybrid' covered entities, where only sections of the organisation must comply with the HIPAA. Universities are an example of this type of entity.[22]

[15] Pascal Coorevits et al, 'Electronic Health Records: New Opportunities for Clinical Research' (2013) 274(6) *Journal of Internal Medicine* 547, 554.

[16] Randike Gajanayake, Renato Iannella and Tony Sahama, 'Sharing with Care: An Information Accountability Perspective' (2011) 15(4) *IEEE Internet Computing* 31, 32.

[17] Dayana Spagnuelo and Gabriele Lenzini, 'Transparent Medical Data Systems' (2016) 41(1) *Journal of Medical Systems* 8, 13.

[18] *Applicability*, 45 CFR § 164.302 (2003); *Security Standards: General Rules*, 45 CFR § 164.306 (2003); *Technical Safeguards*, 45 CFR § 164.312 (2003).

[19] *Definitions*, 45 CFR § 164.103 (2003).

[20] Ibid.

[21] Ibid.

[22] Lorna L Hecker and Anne B Edwards, 'The Impact of HIPAA and HITECH: New Standards for Confidentiality, Security, and Documentation for Marriage and Family Therapists' (2014) 42(2) *The American Journal of Family Therapy* 95, 96.

All entities subject to the HIPAA are required to implement security measures for health information management, including access controls and audit controls.[23] For access control, unique user identification and emergency access procedures are mandatory, whereas automatic logoff and encryption are optional. Audit controls can be implemented using either hardware, software, or procedural mechanisms to record and examine activity in health information systems.[24]

The documentation standards under the *Security Rule* require covered entities or business associates to retain documentation of any action, activity or assessment for six years.[25] Unfortunately, neither the HIPAA nor the *Security Rule* provide guidance as to whether events logged in audit trails should be considered 'documentation'. However, National Institute of Standards and Technology ('NIST') standard NIST SP 800-66 reiterates the requirement for documentation to be retained for at least six years.[26] Further, NIST SP 800-92, in referring to NIST SP 800-66, associates the documentation requirement with performing regular reviews of audit logs and access reports. These standards suggest that events which occur in an information system that stores electronic protected health information are to be considered 'activities' under the HIPAA.[27] Nevertheless, in 2017, the Department of Health and Human Services issued a newsletter on the use of audit logs for cyber security. This newsletter does not explicitly mention that audit logs should be retained for six years. Further, the newsletter does not address the question of how frequently audit logs should be reviewed or what information should be collected as part of the audit trail.[28] It should therefore be assumed that covered entities and business associates must determine how long records should be retained for as part of a contextual risk-based approach.[29]

The question of audit trails also arises in relation to how covered entities can use protected health information. Under the HIPAA and the *Security Rule*, use of

[23] *Technical Safeguards* (n 18).

[24] Ibid.

[25] *Policies and Procedures and Documentation Requirements*, 45 CFR § 164.316 (2003).

[26] Matthew Scholl et al, *An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule* (National Institute of Standards and Technology Special Publication 800-66 Revision 1, 23 October 2008) 19, 52 <https://csrc.nist.gov/publications/detail/sp/800-66/rev-1/final>.

[27] Doug Kanney, 'HIPAA Audit Log Retention Requirements — Do I Really Need to Retain All My Audit Logs for 6 Years?', *Schellman & Company* (Web Page, 11 April 2019) <https://schellmanco.com/>.

[28] Office for Civil Rights, 'Understanding the Importance of Audit Controls', *HHS.gov* (Text, January 2017) <https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity/cybersecurity-newsletter-archive/index.html>.

[29] Kanney (n 27).

patient material for research purposes requires consent from the patient,[30] but use for purposes related to public health does not. The HIPAA also grants patients the right to access their own protected health information in an electronic format. [31] These provisions do not explicitly state whether the data available to patients includes audit trails. However, only psychotherapy notes and material compiled in reasonable anticipation of civil or criminal proceedings can be excluded from access requests.[32] Therefore, it is likely that the material accessible by patients will include audit logs.

2.3 Australia

Australian health privacy legislation operates on overlapping jurisdictional levels, as healthcare (and accompanying legislation regarding health records) is a joint responsibility of the federal Commonwealth and state governments. The Commonwealth government is responsible for funding healthcare services (pursuant to sections 51(xxiiiA), 81 and 96 of the *Commonwealth Constitution*).[33] Therefore, the federal *Privacy Act 1988* (Cth) applies to the health record systems of private hospitals, specialists, and general practitioners. However, state governments also provide state-based healthcare services, such as state hospitals. These services are regulated by state law, which contain provisions on privacy and use of information.[34]

Auditability requirements can be implied from the Health Privacy Principles underpinning legislation for EHRs in the Australian Capital Territory ('ACT'), New South Wales ('NSW') and Victoria. Each State's legislation mandates the use of security measures and access controls to protect health information. Specifically, Health Privacy Principles require healthcare providers to protect health data from unauthorised access, disclosure or erasure. Healthcare providers must also ensure patients can access information about where their records are stored, whether those records are accessible, and for what purposes they are used.[35] The ACT, NSW and Victorian legislation also mandate medical records be kept for up to seven years.[36] However, as for equivalent provisions

[30] *Uses and Disclosures for Which an Authorisation Is Required*, 45 CFR § 164.508 (2003).

[31] *Access of Individuals to Protected Health Information*, 45 CFR § 164.524 (2003).

[32] Ibid.

[33] Karen Wheelwright, 'Commonwealth and State Powers in Health — A Constitutional Diagnosis' (1995) 21(1) *Monash University Law Review* 53.

[34] *State laws include Health Services Act 2016* (WA); *Health Services (Information) Regulations 2017* (WA); *Information Act 2002* (NT); *Information Privacy Act 2009* (Qld); *Personal Information Protection Act 2004* (Tas); *Health Care Act 2008* (SA).

[35] *Health Records (Privacy and Access Act) 1997* (ACT), principle 5 ('ACT Act'); *Health Records and Information Privacy Act 2002* (NSW), principle 6 ('NSW Act'); *Health Records Act 2001* (Vic), s 19, principle 4 — Data Security and Data Retention ('Victorian Act').

[36] ACT Act (n 35) principle 4.2; NSW Act (n 35) s 25; Victorian Act (n 35) s 19, principle 4 — Data Security and Data Retention.

under the HIPAA and the *Security Rule*, it is unclear whether these provisions require retaining audit logs about the use of patient information. Of the three jurisdictions, only the NSW legislation directs health service providers to retain information about records after they are deleted.[37] Finally, the NSW and Victorian legislation permit that data may be used and disclosed for research purposes without consent. Nevertheless, use and disclosure may only occur if it would be impracticable to seek consent and the individual's identity cannot be otherwise determined from the medical records.

At the federal level, the *Privacy Act 1988* imposes security obligations equivalent to those in state regimes on entities processing personal data. Specifically, the *Privacy Act* permits lawful access to data on the Pharmaceutical Benefits Scheme ('PBS') and Medicare Benefits Scheme (MBS) without consent. This can include the release of health-related data to police where there is a particular risk to the health or safety of the patient or another person.[38]

In addition, the federal government has introduced the My Health Record system, the previously-mentioned national summary care record for sharing data associated with healthcare recipients.[39] The My Health Record system is managed by the System Operator, a statutory appointment responsible for arranging computer programs to run the My Health Record system. These computer systems must contain audit logs of system activity and allow healthcare recipients to view and control their access list.[40] These records are visible as an 'access trail' that is updated every time a healthcare recipient's records are accessed, changed, or removed. Nevertheless, as Mendelson and Wolf note, this audit record is only visible to the healthcare recipient. Further, healthcare recipients have the unilateral power to remove documents from their My Health Record.[41] Accordingly, it is possible that, once a healthcare recipient has deleted these documents, healthcare providers will not be able to see that these documents existed if they did not author them.[42] Nevertheless, there is

[37] NSW Act (n 35) s 25.

[38] Felicity Nelson, 'Australian Government Secretly Releasing Sensitive Medical Records to Police', *The Guardian* (online, 26 January 2020) <https://www.theguardian.com/world/2020/jan/27/australian-government-secretly-releasing-sensitive-medical-records-to-police>.

[39] Judith Allen-Graham et al, 'Electronic Health Records and Online Medical Records: An Asset or a Liability under Current Conditions?' (2018) 42(1) *Australian Health Review* 59.

[40] *My Health Records Act 2012* (Cth) s 15(b)–(g); Grant Hehir et al, *Implementation of the My Health Record System* (Auditor-General Report No 13 of 2019–2020) 16–17 <https://www.anao.gov.au/work/performance-audit/implementation-the-my-health-record-system>.

[41] *My Health Record Rules 2016* (Cth) rr 5(b)–(e), 6(1).

[42] Danuta Mendelson and Gabrielle Wolf, '"My [Electronic] Health Record" — Cui Bono (for Whose Benefit)?' (2016) 24(2) *Journal of Law and Medicine* 283, 292; 'My Health Record System Security', *Australian Digital Health Agency* (Web Page)

evidence that only a limited number of patients with My Health Records are using these access control features, possibly reflecting limited patient concerns.[43]

The *My Health Records Act 2012* (Cth) does not specify for how long the System Operator must maintain these audit logs. Records uploaded to the National Repositories Service must be maintained for up to 30 years after the death of the healthcare recipient.[44] However, it is not clear in either the *My Health Records Act 2012* or the *My Health Records Rules 2016* whether this definition of 'records' includes audit logs compiled by the System Operator. Accordingly, in concert with the right of healthcare recipients to erase their records, the My Health Record legislative framework introduces new ambiguities as to the completeness and auditability of summary patient records. Although the *My Health Records Act 2012* heightens obligations beyond those imposed by the *Privacy Act 1988*, the System Operator remains bound by the *Privacy Act*.[45] Further, the *Privacy Act* is currently undergoing revision, so it is possible that the obligations imposed on the use of healthcare records for research may change in the future.[46]

2.4 The European Union

The European Commission introduced the *General Data Protection Regulation* ('GDPR') in 2018 to replace the former *Data Protection Directive* ('DPD'). Although the GDPR is a regulation, meaning its provisions apply directly to national law, most EU member states have modified their legislation to achieve compliance.[47] The GDPR clarifies many of the rights that are available to data subjects under EU data protection law. This includes the right for data subjects to gain access to their data as well as information on how their data have been processed.[48] In

<https://www.myhealthrecord.gov.au/for-healthcare-professionals/howtos/my-health-record-system-security>.

[43] Zachary Hollo and Dominique E Martin, 'An Equitable Approach to Enhancing the Privacy of Consumer Information on My Health Record in Australia' [2021] *Health Information Management Journal* 18333583211019764; Patrick Cheong-Iao Pang et al, 'Privacy Concerns of the Australian My Health Record: Implications for Other Large-Scale Opt-out Personal Health Records' (2020) 57(6) *Information Processing & Management* 102364, 11.

[44] If the death date of the patient is known. If the death date of the patient is not known, records uploaded to the MyHealth Records system must be retained for 130 years after the date of the patient's birth: *My Health Records Act 2012* (Cth), s 17(2)(b)(ii).

[45] *My Health Records Act 2012* (Cth) ss 72–73B.

[46] 'Review of the *Privacy Act 1988*', *Attorney-General's Department* (Web Page) <https://www.ag.gov.au/integrity/consultations/review-privacy-act-1988>.

[47] These include the United Kingdom, which exited the EU on 31 January 2020.

[48] *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regards 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 L 119/1, arts 13, 14, 15 ('*GDPR*').

particular, the right to gain information on processing imposes an implicit requirement on data controllers and processors to supply records of processing when data subjects request this information. Further, the GDPR introduces new data subject rights, including the right to rectify data, to be forgotten, to transfer data to another processor (data portability), and to object to processing.[49] We consider these new rights in the second section of our paper with respect to how they might influence auditability measures.

The GDPR also raises obligations on data controllers and processors to ensure the security of data, particularly special categories of personal data such as health-related and genetic data. These obligations include requiring data protection by design and default, the maintenance of records of processing, mechanisms to support secure processing, and reporting of breaches to data subjects.[50] In addition, the GDPR requires data controllers to implement processes for regularly testing the effectiveness of technical measures for protecting the security of processing.[51] This requirement does not specify exactly how frequently these records should be maintained. However, it is an overarching principle in the GDPR that data should only be kept for as long as necessary for processing.[52]

In concert with the principle of accountable data processing,[53] the need for regular testing imposes on data processors a requirement for auditability.[54] This requirement is more specific than that supplied under the United States' *Security Rule.* It should be further noted that the scope of personal data protected under the GDPR is significantly broader than that under the HIPAA. Further, under the GDPR, explicit consent is required for the ongoing use of special categories of personal data by default, unless another lawful ground for processing applies. These exceptions can include processing for preventative or medical treatment, for public health management, or for scientific research or statistical purposes (subject to technical and organisational safeguards).[55] In addition to a lawful ground for processing, the default position is that personal data can only be processed for a purpose compatible with the purpose for which it was collected.[56]

Since the introduction of the GDPR, there has been no case law regarding the requirements for privacy by design for EHRs. However, article 9(4) of the GDPR

[49] Ibid arts 16, 17, 20, 21.

[50] Ibid arts 25, 30, 32, 33, 34.

[51] Ibid art 32(1)(d).

[52] Ibid art 5(1)(e).

[53] Ibid art 5(2).

[54] Laurence Diver and Burkhard Schafer, 'Opening the Black Box: Petri Nets and Privacy by Design' (2017) 31(1) *International Review of Law, Computers & Technology* 68, 84.

[55] *GDPR* (n 48) arts 9(2)(h), 9(2)(i), 9(2)(j).

[56] *GDPR* (n 48) art 5(1)(b).

allows member states to introduce separate rules for the processing of genetic, health-related and biometric data, including limits on processing. As the EU has encouraged its member states to introduce EHRs for patient data,[57] some states have introduced their own national laws on auditing EHRs. Some jurisdictions mandate specific audit requirements for EHR storage systems (as well as for electronic systems more broadly). For example, in Estonia, Finland, France, Lithuania, Slovenia, and Spain, databases must be audited every two or three years.[58] Other jurisdictions such as Portugal mandate that regular backups and checks on processing must be maintained.[59] In addition, Swedish legislation mandates that quality standards should be maintained, and that audit records should be retained for up to ten years.[60]

Before the GDPR was passed, the former Article 29 Working Party (now the European Data Protection Board) provided guidance in 2007 on privacy protection for data processing in EHRs. This Working Paper recommended that detailed audit trails of patient consent be collected, and that any audit mechanisms be reviewed regularly.[61] Simultaneously, the European Commission also supported the European Patients Smart Open Services project ('epSOS') for cross border e-Health services in the EU. As part of assessing data protection

[57] Patrick Kierkegaard, 'Electronic Health Record: Wiring Europe's Healthcare' (2011) 27(5) *Computer Law & Security Review* 503, 505–8.

[58] *Regulation on System of Security Measures for Information Systems* (Estonia) 25 January 2009 §91(1); *Laki sosiaali – ja terveydenhuollon asiakastietojen sähköisestä käsittelystä* [Act on the Electronic Processing of Client Data in Social and Health Care Services] (Finland) 9 February 2007, No 159, ss 19(a)–(i); *Statute of Health Information System* (Estonia) 24 July 2009 § 6(2); *Public Health Code, Decree No 2003-462 of 21 May 2003 (France)* JO, R.1111-11; *Law on Management of State Information Resources* (Lithuania), 15 December 2011, art 14; *Zakon o varstvu dokumentarnega in arhivskega gradiva ter arhivih – ZVDAGA, št. 30/06 z dne 23.3.2006* [Protection of Documents and Archives and Archival Institutions Act, No 30/06 of 23 March 2006] (Slovenia), art 21; *Real Decret 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica* [Royal Decree 3/2010, of 8 January, regulating the National Security Framework in the area of e-Government] (Spain), arts 34(1), 34(5); *Real Decreto 1720/2007 die 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal* [Royal Decree 1720/2007, of 21 December, which approves the regulations implementing the organic law 15/1999 of 13 December of protection of personal data] (Spain), art 96; *Ley 16/2003, de 28 de mayo, de cohesion y calidad del Sistema Nacional de Salud* [Law 16/2003, of May 28, Cohesion and Quality of the National Health System] (Spain), arts 28, 63, 76.

[59] *Lei no. 12/2005 de 26 de Janeiro Informação genética pessoal e informação sobre saúde* [Law no 12/2005 of 26 January 2005 on Personal Genetics and Health Information] (Portugal), art 4(6).

[60] *Patientdatalag* [Patient Data Law] (Sweden), 2008:355, ch 4, s 3.

[61] Article 29 Data Protection Working Party, *Working Document on the Processing of Personal Health Data Relating to Health in Electronic Health Records (EHR)* (Working Paper No 131, 15 February 2007), 15, 20–1.

requirements for the project, the Article 29 Working Party required project partners to implement audit requirements for health information systems. Specifically, these audit requirements included tracking individual operations in an auditable way and recording any 'risky or non-standard behaviour'.[62] These documents do not provide any further requirements for how often audit logs should be measured. Nevertheless, they indicate what an audit system should entail to comply with European data protection law and they have also been used for other projects involving sharing patient data.[63]

2.5 Switzerland

Switzerland is a federal republic composed of 26 cantons (federated states), each of them having a permanent constitutional status and high degree of independence. Two Swiss cantons, Geneva and Valais, have legislation governing patient electronic dossiers.[64] These acts are reinforced by federal legislation. These include the *Bundesgesetz über den Datenschutz* (Federal Act on Data Protection ('FADP')) and the *Verodnung zum Bundesetz über Datenschutz* (Ordinance to the Federal Act on Data Protection ('OFADP')). These laws were introduced to fulfil Switzerland's obligations pursuant to Council of Europe *Convention 108*.[65]

In 2017, the Swiss Bundesrat introduced the *Bundesgesetz über das elektronische Patientendossier* (Federal Act on the Electronic Patient Records (the 'EPR Act')). The EPR Act mandates that all hospitals and rehabilitation clinics in Switzerland implement infrastructure for interoperable EHRs.[66] However, participation is voluntary for outpatient health facilities such as family doctors, specialists and

[62] Article 29 Data Protection Working Party, *Working Document 01/2012 on epSOS* (Working Paper No 189, 25 January 2012).

[63] Nadezhda Purtova, Eleni Kosta and Bert-Jaap Koops, 'Laws and Regulations for Digital Health' in Samuel A Fricker, Christoph Thümmler and Anastasius Gavras (eds), *Requirements Engineering for Digital Health* (Springer International Publishing, 2015) 47, 52 <https://doi.org/10.1007/978-3-319-09798-5_3>; Ed Conley and Matthias Pocs, 'GDPR Compliance Challenges for Interoperable Health Information Exchanges (HIEs) and Trustworthy Research Environments (TREs)' (2018) 14(3) *European Journal of Biomedical Informatics* 56 <https://www.ejbi.org/abstract/gdpr-compliance-challenges-for-interoperable-health-information-exchanges-hies-and-trustworthy-research-environments-tre-4619.html>.

[64] Effy Vayena et al, 'Digital Health: Meeting the Ethical and Policy Challenges' (2018) 148 *Swiss Medical Weekly* w14571, 6.

[65] *Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data*, opened for signature 28 January 1981, CETS 108 (entered into force 1 October 1985).

[66] *Bundesgesetz über das elektronische Patientdossier* [Federal Act on Electronic Patient Records] (Switzerland) 15 April 2017, SR 816.1, art 16 ('*EBDG*').

other healthcare providers.[67] The EPR Act also creates an opt-in model of consent, as opposed to Australia's opt-out model for the My Health Record system.[68] The patient is then able to determine who can access their data and what levels of data are accessible by different physicians,[69] except for emergency purposes.[70]

As for security requirements, the EPR Act obliges healthcare organisations to maintain a record of any processing of patient data.[71] However, the EPR Act does not explicitly mention the need for healthcare organisations to maintain a temporal record of data processing. Further, it does not indicate how long these records must be retained. Meanwhile, the OFADP requires data controllers to maintain records of automated processing for at least one year if preventative measures cannot support data security.[72]

However, neither the EPR Act nor the OFADP provide a specific requirement on how frequently audit logs should be reviewed. Accordingly, an approach to auditability based on organisational responsibility exists in Switzerland as it does in the US. Nevertheless, as discussed below, the Swiss Parliament passed the revised Federal Act on Data Processing (the 'revFADP'), a new data protection law to comply with recent supranational changes.[73] In particular, article 17 of this revised law permits use and disclosure of data if it is necessary to protect the life or physical integrity of the data subject. Further, article 12 requires data processors and controllers to keep an up-to-date list of data processing activities.[74] This transparency requirement aligns the revFADP with the GDPR and the Council of Europe requirements on data processing, which we will discuss next.

[67] 'Introduction of the Electronic Patient Record — Federal Office of Public Health' Eidgenössische Finanzkontrolle [Swiss Federal Audit Office] (Web Page, 29 June 2020) <https://www.efk.admin.ch/en/publications/training-and-social-affairs/health/3870-introduction-of-the-electronic-patient-record-federal-office-of-public-health.html>.

[68] *EPDG* (n 66) art 3.

[69] Ibid art 9(3)–(4).

[70] Ibid art 9(5).

[71] Ibid art 10.

[72] *Verordnung zum Bundesgesetz über den Datenschutz* [Ordinance to the Federal Act on Data Protection] (Switzerland) 16 October 2012, 235.11, art 10 ('*VDSG*').

[73] Morris Naqib, 'Update on the Revision of the Swiss Federal Act on Data Protection', *PwC* (Web Page, 8 March 2019) <https://www.pwc.ch/en/insights/fs/swiss-federal-act-on-data-protection-revision.html>.

[74] 'The New FADP from the FDPIC's Perspective', Federal Data Protection and Information Commissioner (FDPIC) (Web Page, 5 March 2021) <https://www.edoeb.admin.ch/edoeb/en/home/aktuell/aktuell_news.html/>.

2.6 The Council of Europe

The Council of Europe's modernised *Convention 108* [75] attempts to create congruence between EU data protection law under the GDPR and Council of Europe law.[76] Specifically, the modernised *Convention 108* replicates many of the data subject rights provided under the GDPR. [77] Further, the modernised *Convention 108* requires data processors and controllers to implement technical measures to ensure compliance with and respect for the fundamental rights of data subjects. As for the GDPR, these provisions could create an implied requirement for data processors and controllers to demonstrate auditability for compliance purposes.

Both the original and modernised *Convention 108* have been accompanied by a series of policy frameworks and proposals. The first of these was Recommendation 97(5) issued by the Committee of Ministers, which extended the reach of the original *Convention 108* to health-related data. Specifically, Principle 9 mandates the need for appropriate technical and organisational measures to protect against accidental loss or destruction of data. These include explicit access control mechanisms to separate different data types from one another — data types include personal identifiers, administrative data, medical data, social data, and genetic data.

In May 2019, the Committee of Ministers issued Recommendation 2019(2) to provide further specific guidance for the management of health-related data. In addition to reiterating data subject rights in *Convention 108*, Principles 13.4 and 13.5 of Recommendation 2019(2) implement requirements for the verifiability and auditability of health-related data. Specifically, Principle 13.4 requires mechanisms to support record integrity, including activity on, changes to, and communication of data. Principle 13.4 also requires access control mechanisms to ensure that only authorised persons can access the data. Principle 13.5 then defines 'auditability' as leading to a system where it is possible to trace any action or modification carried out to identify the author. Although the requirements from neither recommendation are binding, they demonstrate a clear advance on the auditability requirements previously present in EU, Swiss, or Council of Europe data protection law. Further, these requirements are more comprehensive than the obligations imposed on the managers of health information systems in the US or Australia.

[75] *Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, opened for signature 18 May 2018, CETS 223.

[76] Jorg Ukrow, 'Data Protection without Frontiers: On the Relationship between EU GDPR and Amended CoE Convention 108 Reports: Practitioner's Corner' [2018] (2) *European Data Protection Law Review (EDPL)* 239, 240.

[77] These include the right to access information about processing, the right to access records (art 9(b)–(c)), and the right to modify or erase inaccurate data (art 9(d)).

A synopsis of the auditability requirements between each of the five jurisdictions discussed above is presented in Table 1.

3 How Can Distributed Ledger Technology Support Lawful Auditability of EHRs?

The analysis of auditability in the five jurisdictions above indicates that there are six shared characteristics of auditability requirements:

- auditing *who* has accessed a particular file or dataset;
- determining *when* it was accessed (the temporal requirement);
- auditing *for what purpose* this file or dataset has been accessed;
- determining *whether this purpose was authorised* or not, or whether consent had been sought;
- what *types of access* had occurred, including creating, reading, writing, modifying or deleting a file or dataset; and
- allowing a patient to audit their own records.

Despite these shared characteristics, there is a significant degree of fragmentation between each of these jurisdictions. In particular, no regime explicitly defines what records are available to be audited and how often audit logs must be kept or inspected. These questions in turn dovetail into how conflicting rights of different stakeholders should be resolved. For example, should a patient's right to control the availability of their documents take precedence over a physician's obligation to provide care? Although unsurprising given that regulation is frequently technology neutral, this finding raises questions about the role that DLT can play in upholding auditability. As Vos notes, the 'first wave' of legal scholarship on smart contracts argued that smart contracts should supplant the existing legal framework.[78] Nevertheless, we submit that for smart contracts to oust existing legal frameworks on patient data, smart contracts must handle disputes and protect patient rights in a legally consistent manner.[79]

[78] Sir Geoffrey Vos, 'End-to-End Smart Legal Contracts Moving from Aspiration to Reality' (2019) 26(1) *Journal of Law, Information & Science*, EAP3 <http://www.jlisjournal.org/abstracts/vos.26.1.html>.

[79] Imran Khan, Moheeb Alwarsh and Javed I Khan, 'A Comprehension Approach for Formalizing Privacy Rules of HIPAA for Decision Support' in *2013 12th International Conference on Machine Learning and Applications* (IEEE Computer Society, 2013) 390, 390; Vlad Zamfir, 'Against Szabo's Law, For a New Crypto Legal System', *Medium* (Blog Post, 25 January 2019) <https://medium.com/cryptolawreview/against-szaboslaw-for-a-new-crypto-legal-system-d00d0f3d3827>.

Table 1: Overview of auditability requirements

Requirements	United States	Australia	European Union (GDPR)	Switzerland	Council of Europe (*Convention 108*)
What records need to be kept?	Covered entities and business associates must log events in health information systems.	Federal – My Health Record The My Health Record System Operator must measure audit activity within the My Health Record system. State (ACT, NSW, Victoria) Audit logs are an implicit requirement alongside access control measures and security protocols. In NSW, a record of processing must be retained after erasure.	Data processors and controllers should implement data protection by design (' DPbD'). These should include mechanisms to report any breaches to data subjects and records of processing. Further, these measures should be tested ' regularly' . Data processing should comply with principles of transparency.	All healthcare providers (although not outpatient providers such as doctors' clinics) must work towards implementing interoperable EHR systems. All processors and controllers must maintain records of processing.	Equivalent to GDPR. Healthcare providers must introduce mechanisms to ensure the integrity of data and access control. Healthcare providers should also introduce audit requirements so that any modification of records can be traced.

How long should these records be retained?	Records must be kept for six years.		Data should only be stored for as long as required for processing. Individual member states may impose additional requirements (for example, Estonia, Finland, France, Lithuania, Slovenia and Spain).	For sensitive data, these records must be retained for at least one year.	Equivalent to GDPR.
When can records be accessed for research?	Patient consent must be sought to use data for research purposes.	*Federal*: Patient consent must be sought for data to be used for research purposes. *State*: Consent is required for scientific research unless it would impose an undue burden on the research.	Patient data can only be used with patient consent or if another grounds for processing applies (public health management, treatment, scientific research).	Records can only be accessed with patient consent or if a waiver has been sought.	Equivalent to GDPR.

Can records be accessed without consent?	Patient consent does not need to be sought for public health research or emergency treatment.	*Federal*: Data cannot be accessed from a patient’s My Health record without a warrant. Data from a patient’s Medical Benefit Scheme /Pharmaceutical can be accessed without a warrant. *State*: Healthcare records may be accessible where it is necessary to protect the safety of that person or another.	Patient data can be accessed without consent if another grounds for processing applies.	May be justified on the grounds of overriding private or public interests or a necessity to comply with a legal obligation made under Swiss law.	Equivalent to GDPR.
Can patients access their own records?	Patients can access health information in electronic format.	*Federal*: Healthcare recipients can access and delete data from their records without recording this deletion in the audit trail. *State*: Patients can access their records at any time.	Data subjects can exercise several rights, including access, information, rectification, erasure, data portability and objections to processing. Data controllers should have mechanisms in place to satisfy these requirements.	Patients can opt into their health records, and are entitled to deny physicians access to these records (except in emergency situations).	Equivalent to GDPR.

We will now address three of the most significant challenges to compliance and dispute resolution in the context of auditability requirements.[80]

3.1 What Can Complicate the Use of DLT for Health Records?

3.1.1 Data Storage

One significant concern with respect to smart contracts and DLT for patient data management is the question of data storage. Part of this concern is attributed to the open and transparent nature of processing for permissionless DLT implementations, where third parties can access sensitive data.

However, different laws provide divergent interpretations of responsibility for joint processing and controllership. Specifically, under Swiss law, controllers must provide information on records being processed by a third party or joint controller,[81] and must ensure third party processors have adequate security.[82] Further, the GDPR provides that two or more controllers who jointly manage processing must determine how data subjects can exercise their right to access their data and information about processing.[83] Data subjects may also exercise their rights under the GDPR equally against each of the controllers.[84]

How this joint controllership will be interpreted by authorities remains unclear, but would require careful governance to ensure compliance with auditability requirements.[85] In particular, a permissionless DLT implementation with open membership would complicate compliance with auditability requirements under data protection laws. In turn, a lack of compliance could expose data processors and controllers to severe financial penalties for data breaches. In this regard, the drafters of the GDPR have stated that '[blockchain], in general, probably can't be used for the processing of personal data'.[86]

[80] William J Gordon and Christian Catalini, 'Blockchain Technology for Healthcare: Facilitating the Transition to Patient-Driven Interoperability' (2018) 16 *Computational and Structural Biotechnology Journal* 224, 228.

[81] *EPDG* (n 66) art 8(4); *VDSG* (n 72) art 1(5).

[82] Ibid art 10a(2).

[83] *GDPR* (n 48) art 26(1).

[84] Ibid art 26(3).

[85] Matthias Berberich and Malgorzata Steiner, 'Blockchain Technology and the GDPR — How to Reconcile Privacy and Distributed Ledgers Reports: Practitioner's Corner' (2016) 2(4) *European Data Protection Law Review (EDPL)* 422, 424.

[86] David Meyer, 'Blockchain Technology Is on a Collision Course with EU Privacy Law' (Web Page, 27 February 2018) <https://iapp.org/news/a/blockchain-technology-is-on-a-collision-course-with-eu-privacy-law/>.

3.1.2 *Privacy and Security*

The question of governance arrangements for processing patient data dovetails into the need to ensure that systems are private and secure. Under Swiss and EU data protection law, the need to audit information systems for storing personal data goes beyond providing patients with information about processing. Rather, it extends to include transparency of processing. Therefore, to fulfil auditability requirements (at least under EU and European law), smart contracts and DLT must ensure that patient records are auditable by both patients and regulatory bodies (namely, national data protection agencies). However, clinical continuity and availability of records might directly clash with the patient's right to control their own records. For example, patients who erase their data could undermine the ability of healthcare providers to provide clinical care, particularly if the healthcare provider is unaware the data has been deleted.[87] Further, the security of the underlying ledger depends on its indelible nature. Accordingly, mandating that data be deleted from the ledger could undermine the overarching security of the ledger.[88] Although exceptions exist under the GDPR for public health and research purposes,[89] these requirements will still need to be interpreted by reference to the relevant national implementation of the GDPR.

3.1.3 *Patient Engagement*

The final key obstacle to compliance with auditability requirements for DLT is encouraging patient engagement. As with any novel technology, public education and awareness are vital. However, as Herian notes, there is a lack of critical education regarding the utility of DLT in both the public and private sector. Further, there remains an open question as to who frames these education campaigns and what purposes they serve.[90] In this regard, the regulatory fragmentation with respect to auditability can have several adverse consequences.

First, the fact that there are multiple definitions and requirements for auditability means that, between jurisdictions, there will be different expectations of auditability. Secondly, within a jurisdiction, there may be varying levels of information technology literacy and computational awareness. Any education

[87] Mendelson and Wolf (n 42) 292; Danuta Mendelson, 'National Electronic Health Record Systems and Consent to Processing of Health Data in the European Union and Australia' in Marcelo Corrales Compagnucci et al (eds), *Legal Tech and the New Sharing Economy* (Springer, 2020) 83, 97; Eugenia Politou et al, 'Backups and the Right to Be Forgotten in the GDPR: An Uneasy Relationship' (2018) 34(6) *Computer Law & Security Review* 1247, 1249.

[88] Robert Herian, 'Regulating Disruption: Blockchain, GDPR, and Questions of Data Sovereignty' (2018) 22 *Journal of Internet Law* 1 and 8 ('Regulating Disruption').

[89] *GDPR* (n 48) art 17(1)(c)–(d).

[90] Robert Herian, *Regulating Blockchain: Critical Perspectives in Law and Technology* (Routledge, 2018) 26, 29.

campaign must not only explain how DLT works from a technical perspective, but also allow patients to reach decisions about the extent to which DLT impacts their lives. Finally, if an education campaign does allow patients to make these decisions, there must be a legal framework in place to support and reinforce their decisions. [91]

Returning to the syllogism we described at the beginning of this section, DLT and smart contract implementations can only replace legal mechanisms for auditability if these requirements are universal. However, as our analysis demonstrates, the auditability requirements between jurisdictions are not uniform. Accordingly, DLT cannot cover the field on auditability requirements for EHRs outside of a defined legal framework. We argue that a combined technical and legal approach is required to guarantee compliance with data protection laws.[92] In the next section, we describe the legal architecture to achieve this goal. Although we do not prescribe the technical architecture required for DLT to be legally compliant, we provide a list of implementations that demonstrate legal compliance.

3.2 Standards and Technical Definitions of Auditability

This section will address the standards and technical architectures for DLT that can comply with and clarify often-implicit legislative auditability requirements at the 'legal layer'. [93] Standards developed by standards setting organisations ('SSOs') such as the International Organisation for Standardisation ('ISO') provide an interface between the technical and legal layers of software development. Accordingly, these standards may provide useful guidance as to the extent of auditability requirements for DLT implementations.[94] These audit standards are described in Table 2.

The ISO has also established a technical committee for blockchain and other DLTs. This working group will focus on use cases, security and privacy concerns, as well as contractual frameworks, but will not address questions of governance and auditability.[95]

[91] Ibid 29.

[92] Jenifer Sunrise Winter and Elizabeth Davidson, 'Governance of Artificial Intelligence and Personal Health Information' (2019) 21 *Digital Policy, Regulation and Governance* 280, 286.

[93] Darra Hofman et al, '"The Margin between the Edge of the World and Infinite Possibility": Blockchain, GDPR and Information Governance' (2019) 29(1/2) *Records Management Journal* 240, 252.

[94] Conley and Pocs (n 63) 52.

[95] Ashiq Anjum, Manu Sporny and Alan Sill, 'Blockchain Standards for Compliance and Trust' (2017) 4(4) *IEEE Cloud Computing* 84, 88.

Table 2: Audit standards for health information systems

Standard	Description
ISO/IEC 27001	Data processors must assess potential risks, ensure the confidentiality of patient data via access control and mandate ongoing monitoring to ensure compliance.[96]
ISO 27789	Data processors must demonstrate a minimum level of event logging with respect to users creating, modify, using or deleting records (without necessarily demonstrating why).[97]

This question of governance and auditability requirements imposed by standards dovetails into technological governance guarantees discussed in the literature. For example, role-based access control ('RBAC') rests on the idea that only authorised users should access confidential data.[98] However, these access control permissions are the least granular of all privacy policies. Specifically, access control satisfies the requirement of recording who has accessed what data, but does not satisfy requirements about recording temporality, location, types, and purposes of access.[99] Therefore, RBAC may not indicate whether all aspects of a privacy policy have been satisfied for audit purposes.[100] In other words, RBAC cannot demonstrate organisational accountability and transparency of processing for controllers and processors of health data as required under data protection law.[101] This paper will now address the three use cases identified in

[96] Georg Disterer, 'ISO/IEC 27000, 27001 and 27002 for Information Security Management' (2013) 4(2) *Journal of Information Security* 95–8.

[97] Chathurika Wickramage, Tony Sahama and Colin Fidge, 'Anatomy of Log Files: Implications for Information Accountability Measures' in *2016 IEEE 18th International Conference on E-Health Networking, Applications and Services (Healthcom)* (IEEE, 2016) 1, 4.

[98] Paul Martin, Aviel D Rubin and Rafae Bhatti, 'Enforcing Minimum Necessary Access in Healthcare Through Integrated Audit and Access Control' in *Proceedings of the International Conference on Bioinformatics, Computational Biology and Biomedical Informatics* (Association for Computing Machinery, 2013) 946, 946–7.

[99] Zheng Zhou and Brent J Liu, 'HIPAA Compliant Auditing System for Medical Images' (2005) 29(2) *Computerized Medical Imaging and Graphics* 235, 235.

[100] Anupam Datta et al, 'Understanding and Protecting Privacy: Formal Semantics and Principled Audit Mechanisms' in Sushil Jajodia and Chandan Mazumdar (eds), *Information Systems Security* (Springer Berlin Heidelberg, 2011) 1, 4.

[101] Aurelia Tamò-Larrieux, 'Technical Tools and Designs for Data Protection' in Aurelia Tamò-Larrieux (ed), *Designing for Privacy and Its Legal Framework: Data Protection by*

the introduction where DLT can help support the auditability of EHRs in a legally compliant manner.

3.3 Auditability and Patient Access and Control

One definition of auditability offered by Spagnuelo and Lenzini is that it is the 'property that allows users to audit what happened to their personal data'.[102] In examining user comments on a *care.data* information website, Sterckx et al highlight patient concerns about their data being misappropriated or commercialised without consent, and their wishes to be included in the research process.[103] Further, patients now generate their own health data using consumer e-Health applications, Internet of Things ('IoT') or Internet of Medical Things ('IoMT') devices, satisfying this ownership and control requirement. These devices challenge existing regulations, as the data they generate is not necessarily sent to a healthcare provider such as a physician or hospital.[104] In particular, Mendelson and Wolf criticise the My Health Record implementation for seeking to provide a complete record of patient information without reckoning against the volume of health data generated by the patient themselves.[105] These devices may also present new threat vectors through which patient health information can be compromised, even if they offer encryption and anonymisation functionalities to protect patient data.[106]

The immutability of the ledger allows a patient to examine all actions that have been performed with their data by a physician, healthcare institute, or researcher. One example of a DLT implementation to improve patient control over their EHRs is MedRec. MedRec uses smart contracts to allow patients to determine access permissions for their medical data. Instead of a public and permissionless ledger, MedRec relies on a private peer-to-peer ledger that operates between patients, providers and insurers. Patients can then form contracts with providers or insurers to grant access. These contracts then help patients trace who has accessed their records and when this access occurred, satisfying the temporal

Design and Default for the Internet of Things (Springer International Publishing, 2018) 101, 141.

[102] Dayana Spagnuelo, Cesare Bartolini and Gabriele Lenzini, 'Qualifying and Measuring Transparency: A Medical Data System Case Study' [2020] *Computers & Security* 101717, 5.

[103] Sterckx et al (n 6) 182–3.

[104] W Nicholson Price and I Glenn Cohen, 'Privacy in the Age of Medical Big Data' (2019) 25(1) *Nature Medicine* 37, 39.

[105] Mendelson and Wolf (n 42) 286.

[106] Rolf H Weber and Evelyne Studer, 'Cybersecurity in the Internet of Things: Legal Aspects' (2016) 32(5) *Computer Law & Security Review* 715, 721.

requirement existing in most jurisdictions.[107] Dubovitskaya et al describe an equivalent implementation where patient data is stored in a cloud repository. The ledger then stores the appropriate access controls for each physician that is accessing the patient's data, with the patient being able to control these access levels via a mobile application.[108]

Both of these implementations satisfy the legal requirements for patients to be able to access information on how and when their data has been processed.

3.4 Auditability and Physician Access to Records

Allowing patients to audit and control access to their records may also challenge the ability of physicians and other healthcare providers to audit records. In the context of EHRs, Fernández-Alemán et al note that one of the three most important aspects of security is ensuring record availability.[109] In particular, patients frequently visit multiple healthcare providers for consultations, or may be transferred to specialist healthcare practitioners for treatment. Further, different healthcare providers frequently have different technical platforms for EHRs. Therefore, as Mendelson and Wolf argued with respect to the My Health Record system, quality of patient care may decline without a complete patient record.[110]

This question of interoperability lies at the heart of concerns over centralised versus decentralised electronic healthcare repositories. On the one hand, centralised systems involve storing patient records in a single location. This approach makes it easier to access those records, but creates a single point of failure or entry for malicious actors, raising the potential liability of custodians.[111] On the other hand, decentralised systems decrease the liability of data custodians by decreasing the number of records they control. However, decentralised systems are undermined by a lack of interoperability between EHRs. A landscape of fragmented standards impedes patient data sharing and collaborative decision making between healthcare institutions, particularly in rural settings.[112]

[107] Asaph Azaria et al, 'MedRec: Using Blockchain for Medical Data Access and Permission Management' in *2016 2nd International Conference on Open and Big Data (OBD)* (IEEE, 2016) 25, 28.

[108] Alevtina Dubovitskaya et al, 'Secure and Trustable Electronic Medical Records Sharing Using Blockchain' (2018) 2017 *AMIA Annual Symposium Proceedings* 650, 655–6.

[109] José Luis Fernández-Alemán et al, 'Security and Privacy in Electronic Health Records: A Systematic Literature Review' (2013) 46(3) *Journal of Biomedical Informatics* 541, 542.

[110] Mendelson and Wolf (n 42) 292.

[111] Dubovitskaya et al (n 108) 651.

[112] Peng Zhang et al, 'FHIRChain: Applying Blockchain to Securely and Scalably Share Clinical Data' (2018) 16 *Computational and Structural Biotechnology Journal* 267, 268.

A recurring focus of DLT implementations for EHRs has therefore been to encourage interoperable data sharing between different institutions. For instance, MedRec utilises an additional technical layer between the ledger and the provider data repository to translate a representation of patient records onto the ledger. This approach harmonises the need for interoperable records between each healthcare provider without replicating each record.[113] Likewise, the FHIRChain architecture is designed to integrate with existing health information systems by storing the patient data outside the ledger. Instead, the ledger contains specific pieces of structured meta data and audit logs associated with access tokens for each patient's health records. These tokens can then be used to access a patient's records using an asymmetric encryption system.[114] Finally, the Estonian government implemented a nationwide ledger-based system in 2011 for validating patient identities for healthcare records stored between healthcare institutions.[115] As with MedRec and FHIRChain, the Estonian e-Health system provides a mechanism for tracking changes to patient records, which are registered in the e-Health ledger.[116] The patient can also view their ledger online, as well as deny and permit access to any case-related data. Crucially, a patient can deny access for research purposes, which satisfies the auditability requirement that patients maintain granular control over the uses of their EHRs.[117] This functionality dovetails into the use case of research purposes, as we discuss in the next paragraph.

3.5 Auditability and Researcher Access to Records

Unlike for clinical treatment where explicit consent for treatment is either present or absent, consent requirements can vary for research uses of information.[118] In particular, any system involving the use of EHRs for research involving identifiable patient data must distinguish between general consent and specific consent. Beyond the need to record patient consent, Manion et al identify three requirements for auditability in multisite research.

First, researchers may reuse data from health records, provided that this data has been sufficiently anonymised or pseudonymised so that individuals may not be reidentified. Accordingly, the audit trail that is visible to researchers cannot

[113] Azaria et al (n 107) 28–9.

[114] Zhang et al (n 112) 276–7.

[115] Oscar Williams-Grut, 'Estonia Is Using the Technology behind Bitcoin to Secure 1 Million Health Records', *Business Insider* (online, 3 March 2016) <https://www.businessinsider.com/guardtime-estonian-health-records-industrial-blockchain-bitcoin-2016-3>.

[116] Suveen Angraal, Harlan M Krumholz and Wade L Schulz, 'Blockchain Technology' (2017) 10(9) *Circulation: Cardiovascular Quality and Outcomes* e003800, 2.

[117] Jaan Priisalu and Rain Ottis, 'Personal Control of Privacy and Data: Estonian Experience' (2017) 7(4) *Health and Technology* 441, 449.

[118] *Rogers v Whitaker* (1992) 175 CLR 479, 490.

attach to individual records, but instead should attach to a particular dataset. To maximise data reuse, a metadata registry of access requests made against a particular dataset should be attached to the dataset. This functionality would satisfy the requirement under data protection law that research be conducted optimally with de-identified or anonymised data.

Secondly, researchers may be accountable to other authorities beyond data protection agencies or government departments. These include the institutional review board ('IRB') or ethics review committee ('ERC') of the institution providing or receiving the data, or the funding agency for a research project. Therefore, an academic audit trail should not only demonstrate compliance with data protection legislation but also the approved study protocol that access is conditioned upon. For determining whether there has been academic malpractice, records of processing may need to be retained for a significantly longer period than in clinical practice.

Thirdly, when data is used for research purposes between organisations, it is necessary to determine the authenticity of a particular dataset. In other words, an audit trail should demonstrate whether the data has been modified or manipulated prior to use.[119]

Accordingly, several DLT implementations include mechanisms for recording access for research. Performing computations on aggregate data can help protect the privacy of individual users by querying aspects about the population under study. In their paper, Dubovitskaya et al describe how aggregated data can be made available for research purposes by tracing consent against a common ledger.[120] Likewise, Froelicher et al describe how a ledger can store access requests for aggregated data. The queries that are stored on this ledger can then be queried by an independent auditor.[121] Finally, on a regional or nationwide level, DLT implementations have been introduced to help resolve concerns posed by misuse of EHRs in research. An example is the collaboration between Google DeepMind and the Royal Free London NHS Foundation Trust. This arrangement was established for developing a smartphone application, Streams, that would be used for treating Acute Kidney Injury. However, an investigation by the UK Information Commissioner's Office revealed that identifiable patient data from the Trust had been transferred to DeepMind without explicit patient consent.[122]

[119] Frank J Manion et al, 'Security and Privacy Requirements for a Multi-Institutional Cancer Research Data Grid: An Interview-Based Study' (2009) 9(1) *BMC Medical Informatics and Decision Making* 31, 25–9.

[120] Dubovitskaya et al (n 108) 653.

[121] David Froelicher et al, 'Drynx: Decentralized, Secure, Verifiable System for Statistical Queries and Machine Learning on Distributed Datasets' [2019] *arXiv:1902.03785 [cs]* 9, 21–2 <http://arxiv.org/abs/1902.03785> ('Drynx').

[122] Julia Powles and Hal Hodson, 'Google DeepMind and Healthcare in an Age of Algorithms' (2017) 7(4) *Health and Technology* 351, 354.

After this, DeepMind introduced Verifiable Audit, a DLT implementation that allowed patients to track the use of their data in Streams research.[123]

3.6 Discussion and Synthesis

As we concluded at the beginning of this section, DLTs cannot supersede the current data protection framework for auditability. Although there is a shift towards standardising data protection laws internationally, we suspect that a degree of divergence in national legislation, particularly for health data, will remain.[124] Further, recent legislative developments in this area support the notion that DLT is subservient to data protection law. For example, draft Swiss legislation on DLT and financial services reserves the right under data protection law to information about how an individual's data has been processed. We also observe that the majority of DLT implementations in healthcare are explicitly designed to comply with, rather than attempt to oust, data protection regimes.

For example, both the MedRec and FHIRChain implementations feature 'off the ledger' storage where data is stored in another location, such as a local repository or a cloud storage service. A pointer or a cryptographic hash reference to the data is then stored on the ledger, allowing data to be queried by clinicians or researchers. Storing the data off the ledger reduces both the risk of access by unauthorised parties and the difficulty in auditing all access. The use of references or cryptographic hashes also allows controllers to comply with erasure requirements without compromising the ledger's integrity.[125]

Further, we submit that these DLT implementations must also be coupled with appropriate organisational solutions. Private or 'permissioned' ledgers operated by a consortium of organisations could be programmed to include appropriate access control and auditability measures.[126]

Finally, public awareness and education campaigns must be structured to provide patients with a meaningful say in the use of their health records. These education campaigns must be explicitly linked to and recognise the regulatory effects of national data protection law on DLT. For example, the UK DeepMind currently claims to support the auditability of EHRs used in research and development via the Verifiable Data Audit DLT. However, after the

[123] Mustafa Suleyman and Ben Laurie, 'Trust, Confidence and Verifiable Data Audit', *DeepMind* (Blog Post, 9 March 2017) <https://deepmind.com/blog/trust-confidence-verifiable-data-audit/>.

[124] Graham Greenleaf, '"Modernising" Data Protection Convention 108: A Safe Basis for a Global Privacy Treaty?' (2013) 29 *Computer Law and Security Review* 430, 436.

[125] Giueseppe Ateniese et al, 'Redactable Blockchain — or — Rewriting History in Bitcoin and Friends' in *2017 IEEE European Symposium on Security and Privacy (EuroS P)* (IEEE, 2017) 111, 114.

[126] Luke Munn, Tsvetelina Hristova and Liam Magee, 'Clouded Data: Privacy and the Promise of Encryption' (2019) 6(1) *Big Data & Society* 2053951719848781, 4.

implementation of this platform, Google announced it would take over DeepMind app development to develop the product commercially. Austin and Lie note that this decision gave Google the capacity to link NHS data with Google data, which Google had previously assured would not happen.[127] This controversy demonstrates the importance of transparency and accountability in processing EHRs, not just as a technical feature, but also as an inherent legal and ethical safeguard. As Powles and Hodson note, any public awareness or education campaign should confirm with patients whether they accept how their data is being processed, either by governments or technology companies.[128]

4 *Conclusion*

In this paper, we examined the potential of DLT and smart contracts to offer auditability for the processing of EHRs. Computer scientists and policy makers have heralded these innovations as general-purpose technologies capable of disrupting many existing processes in healthcare and research. This includes disrupting how health information systems are managed and offering an audit trail of use and disclosure of health information. Some technical and legal scholars have separately argued that DLT and smart contracts offer the potential to supersede existing legal arrangements, particularly in contract law. However, we argue that a similar approach to DLT for auditability and EHRs is unviable. In section 1, we show that there exists both fragmentation and uncertainty in auditability requirements under legal regimes for data protection in five jurisdictions: the US, Switzerland, Australia, the EU, and the Council of Europe. These divergences concern how long audit data should be retained, what access is protected, and whether patients should be entitled to edit their own records.

Because of these uncertainties, we do not accept that a technological solution such as DLT implementations can entirely oust the existing legal framework. Existing controllership requirements, security obligations, and the likelihood of patients opting out mean that a purely technical solution is unviable for resolving concerns regarding auditability. Instead, we submit that a combination of law, standards, and technical solutions must be used to build a best practice framework for auditability with respect to patient health data.

In addition, we argue that there are three main use cases where DLT can aid with improving the management of EHRs. These use cases are: enabling patient control over health records, improving clinical continuity, and aiding research projects. In each of these use cases, the immutability and traceability that is inherent in DLT can offer an increased granularity of control and auditing. Nevertheless, any DLT implementation must be designed so as to comply with

[127] Lisa M Austin and David Lie, 'Safe Sharing Sites' (2019) 94(4) *New York University Law Review* 581, 587.

[128] Julia Powles and Hal Hodson, 'Response to DeepMind' (2018) 8(1) *Health and Technology* 15, 15.

the rights and responsibilities assigned under data protection or electronic health record law. Further, a DLT implementation should be accompanied by a governance framework that clearly highlights the responsibilities of each controller over the legislation. These measures are necessary so that patients, physicians, and researchers can rely on the auditability of the ledger. Finally, all stakeholders should be made aware of the use of DLT for EHR management and how it affects their rights and responsibilities.