
Article:
Basu, S orcid.org/0000-0001-5863-854X and Guinchard, A (2020) Restoring Trust into the NHS: promoting data protection as an 'architecture of custody' for the sharing of data in direct care. International Journal of Law and Information Technology, 28 (3). pp. 243-272. ISSN 0967-0769

https://doi.org/10.1093/ijlit/eaaa014

Restoring Trust into the NHS: promoting data protection as an 'architecture of custody' for the sharing of data in direct care

Subhajit Basu (University of Leeds) & Audrey Guinchard (University of Essex)

Abstract

Aiming to provide better, more personalised care, by harnessing the power of digitalisation, the National Health Service (NHS) has employed a strategy of sharing its patients' information with the private sector, raising questions as to whether it can be trusted as a custodian of its patients' data. The development of the Streams application by DeepMind, a subsidiary of Google Health UK, illustrates the dichotomy between, on the one hand, the need to use innovative technologies to provide effective direct care and, on the other hand, the obligation to protect patients' rights and interests in their health data.

This paper focuses on an under-explored aspect of the Streams debate: the NHS's processing of health data in direct care. It argues that the data protection framework is best viewed as an architecture of custody, where all participants in the framework have a custodial role to play and should collaborate to ensure the balance between the free flow of data and the data subjects' rights and interests.

1. Introduction

Aiming to provide better, more personalised care, by harnessing the power of digitalisation, the National Health Service (NHS) has employed a strategy of sharing its patients' information with the private sector, raising questions as to whether it can be trusted as a custodian of its patients' data. In order to innovate,[1] the NHS has to bring third-party contractors, with the danger that long-standing attitudes to technological development have often been detrimental to strong privacy and security by design. The NHS has thus to balance two competing objectives and duties: the need to use innovative technologies and share data to improve care; its obligation to protect patients' rights and interests in their health data.[2] The NHS asked DeepMind, a British AI company, now absorbed in Google Health UK,[3] to build and test Streams, a smartphone app to help clinicians managing acute kidney injury (AKI), a health condition that can lead to the patient's death if not detected and treated early.[4] The revelations as to the massive data-sharing agreement between

[1] The Covid-19 pandemic highlights the same need to out-source the development of innovative digital solutions, with the added dimension of the NHS managing a public health crisis. See House of Commons, Science and Technology Committee, Oral evidence, UK Science, Research and Technology Capability and Influence in Global Disease Outbreaks, HC 136, Q 354.

[2] On duty to share while complying with the law of confidence and data protection, s251B of the Health and Social Care Act 2012 Added by s3 of the Health and Social Care (Safety and Quality) Act 2015. See notably M Taylor 'Confidentiality and data protection' in J Laing, J McHale, I Kennedy & A Grubb (eds.) *Principles of Medical Law*. (4 edn, Oxford University Press 2017) 672, para 12.103

[3] Rory Celland-Jones, 'Google swallows DeepMind Health', BBC 18 September 2019 at https://www.bbc.co.uk/news/technology-49740095 accessed 24 January 2020

[4] Hal Hodson, 'Revealed: Google AI has access to huge haul of NHS patient data', Newscientist 29 April 2016 at https://www.newscientist.com/article/2086454-revealed-google-ai-has-access-to-huge-haul-of-nhs-patient-data/#ixzz6LUL66vQj

the NHS and DeepMind came as a shock,[5] and concerns about the lawfulness and ethics of the processing have marred the project in controversy. Criticisms have ranged from privacy violations to issues related to the right to health, as well as to the ethics and governance in view of Google's potential market monopoly on big data.[6]

This paper focuses on an under-explored aspect of the Streams debate: the NHS's processing of health data in direct care, under initially the Directive 95/46/EC,[7] as transposed by the UK Data Protection Act 1998 (DPA1998),[8] and since 25 May 2018, under the General Data Protection Regulation (GDPR)[9] and the UK Data Protection Act 2018. To strike the right balance between the free flow of data and the rights of the data subjects as per Article 1 GDPR and former Directive, we propose to view the data protection framework as an 'architecture of custody'. We demonstrate by using Streams as an example, how each participant of the framework has inherent custodial duties towards the data, whether the participant decides to process (controllers) or execute the processing (processors), or is the patient as data subjects, third-party citizens, or regulatory authorities.

In 2016, the sharing of 1.6 million patients' health data underlying the testing of the Streams application, developed by DeepMind at Royal Free NHS London Foundation Trust's request, was found in violation of healthcare ethical guidance, for lack of transparency. [10] Six months later, in July 2017, the Information Commissioner Office (ICO), the UK data protection regulator, found Royal Free in violation of the DPA1998 because of the Trust's lack of transparency and inability to justify the processing and demonstrate its proportionality.[11] These findings did not seal the fate of the project. Instead, the ICO signed an undertaking with Royal Free for the Trust to ensure future compliance, complete a privacy impact assessment and commission an external audit. Two years later, the app has become an integral part of direct care at Royal Free; its use extended to two additional UK hospitals.[12] In July 2019, the ICO concluded that Royal Free now complies with the GDPR and the UK DPA 2018. Nevertheless, without attracting much attention,[13] other extensions projects have

[5] J Powles and H Hodson, 'Google DeepMind and Healthcare in an Age of Algorithms' (2017) 7 *Health and Technology* 351-367,
[6] Ibid.
[7] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals regarding the processing of personal data and on the free movement of such data, OJ L 281, 23/11/1995, p.31-50, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:31995L0046
[8] Data Protection Act 1998 c.29, now repealed by the Data Protection Act 2018 c. 12
[9] 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; in the UK, the Data Protection Act 2018 complements the GDPR.
[10] Letter from the National Data Guardian to Royal Free of 16 December 2016, and previously letter from the National Data Guardian to the Information Commissioner, 12 October 2016, at https://www.gov.uk/government/publications/request-for-information-about-royal-frees-work-with-deepmind
[11] See the letter outlining the conclusions of the ICO's investigation 3 July 2017 https://ico.org.uk/media/action-weve-taken/undertakings/2014353/undertaking-cover-letter-revised-04072017-to-first-person.pdf;'
[12] The Barnett Hospital, under the Royal Free Trust; Imperial College Healthcare NHS Trust (Imperial College) at https://www.digitalhealth.net/2019/01/imperial-deepminds-streams-app/ and the rollout was announced on 21 January 2019, see https://www.imperial.nhs.uk/about-us/news/new-technology-partnership-to-help-patient-safety-and-care
[13] Concerns focused on the absorption of DeepMind by Google Health UK announced in November 2018, see notably Alex Hern, 'Google "betrays patient trust" with DeepMind Health move', The Guardian 14 November 2018, at https://www.theguardian.com/technology/2018/nov/14/google-betrays-patient-trust-deepmind-healthcare-move. The absorption was finalised in September 2019 (n 1)

been paused,[14] with notably one Trust not renewing its contract with DeepMind on the basis that the Streams app was not necessary to its patients' care, an assessment strikingly opposite to that of Royal Free, despite the app serving the same objective: to assist clinicians in the prevention of acute kidney injury (AKI).[15]

The initial criticisms of the DeepMind project[16] feed into broader ethical and legal concerns: firstly, the challenges associated with health data governance in public-private partnerships;[17] secondly, how asymmetries of powers and information between individuals and those processing their data can undermine individuals' ability to control the sharing of their health data for themselves and the broader societal good; [18] and finally, the wider debate currently developing on the need of a 'duty of care' in the data protection framework as recommended by the Joint Committee on Human Rights.[19] While patients have become more alert to the benefits that sharing their health data bring,[20] they are also generally concerned by 'a lack of transparency and awareness around the use of data, making it difficult to secure public trust'.[21] Not getting the balance right may lead to projects being abandoned, such as NHS care.data scheme.[22]

From a data protection law perspective, these questions are neither specific to the healthcare sector nor novel. To deal with these asymmetries of powers and information, and thus re-instate a balance between individuals (data subjects), and data controllers, data protection laws have emphasised individuals' effective control on the processing, although without elevating this control to a principle or a right to

[14] Yeovil District Hospital NHS Foundation Trust (Yeovil), at https://deepmind.com/blog/bringing-streams-yeovil-district-hospital-nhs-foundation-trust/ and at https://yeovilhospital.co.uk/new-mobile-app-will-improve-patient-care/; Taunton and Somerset NHS Foundation Trust (Taunton), at https://www.tsft.nhs.uk/patients-and-visitors/confidentiality-and-data-protection/

[15] Yeovil refused to renew the contract (n 14); J Oates, 'Five NHS trusts do DeepMind data deal with Google. One says no', The Register 19 September 2019 at https://www.theregister.co.uk/2019/09/19/five_nhs_trusts_do_data_deal_with_google_one_says_no/

[16] J Powles and H Hodson (n 5)

[17] J Winter and E Davidson, 'Big data governance of personal health information and challenges to contextual integrity', (2019) 35(1) The Information Society 36; and more broadly, T Sharon, 'When digital health meets digital capitalism, how many common goods are at stake?' (2018) Big Data & Society 1.

[18] D Caldicott, *Information: To share or not to share. Information Governance Review* (Department of Health, 2013); D Caldicott, *UK National Data Guardian, Review of Data Security, Consent and Opt-Outs,* (Department of Health, 2016), available at: https://www.gov.uk/government/publications/review-of-data-security-consent-and-opt-outs; NDG, Reasonable expectations: supporting health and care professionals to share data in line with patient expectations October 2017 – report, At https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/742947/830_-_Supporting_health_and_care_professionals_to_share_data_in_line_with_patient_expectations_-_October_2017_seminar_FINAL.pdf. Article 29 WP *Working Document on the processing of personal data relating to health in electronic health records (EHR)* WP 131 (2007)

[19] *The Right to Privacy and the Digital Revolution*, 2019, Recommendation 33, page 37 at https://publications.parliament.uk/pa/jt201919/jtselect/jtrights/122/122.pdf

[20] European Alliance for Personalised Medicine Innovation and Patient Access to Personalised Medicine'<http://euapm.eu/pdf/EAPM_REPORT_on_Innovation_and_Patient_Access_to_Personalised_Medicine.pdf> accessed 24 January 2020.

[21] European Alliance (n20); Spencer K and others, 'Patient Perspectives on Sharing Anonymized Personal Health Data Using a Digital System for Dynamic Consent and Research Feedback: A Qualitative Study' (2016) 18 (4) *Journal of Medical Internet Research*; see also M Taylor, 'Legal bases for disclosing confidential patient information for public health: distinguishing between health protection and health improvement' (2015) 23(3) *Medical Law Review* 348, 350 fns 7 and 8.

[22] In 2015, the Secretary of State commissioned the National Data Guardian to undertake a third review, which was tasked with recommending a new national opt-out model for health and social care data. Following the publication of the review, NHS England announced formally that care.data would be stopped, after being indefinitely paused since 2014, see National Data Guardian 2016 (n18)

informational self-determination.[23] The EU Directive, as interpreted by the Court of Justice, [24] has indeed aimed to ensure data subjects exercise their rights to challenge those taking decisions on processing in terms of necessity and proportionality. [25]

Nevertheless, the inherent danger of emphasising individuals' control is to expect too much from the data subjects, and not enough from the other key participants in the framework: controllers, processors, and data protection authorities.[26] As a remedy, some have suggested other avenues, such as property rights and data trusts.[27] Others proposed to view this 'architecture of control'[28] as a 'normative anchor' in interpreting the data protection framework, a lens through which the responsibilities of controllers can be interpreted and balanced, and supervision and enforcement conducted. [29] The GDPR certainly does not just reinforce and extend the data subjects' rights existing under the Directive.[30] For data subjects to remain in control of their data, it promotes stronger enforcement from data protection authorities, greater transparency and accountability from data controllers and processors, and allows for third-parties' complaints against data controllers.[31]

While this 'architecture of control' is to be lauded for its emphasis on not leaving individuals alone in protecting their data, we argue that the terminology of 'control' and 'controllers' tends to encourage viewing the responsibility either of the individual or the controller and often in opposition to each other. It does not facilitate a systematic perception that balancing competing rights and interests is a

[23] The OECD guidelines refer to an Individual participation principle, but the text remains an exception, L. Bygrave, *Data Privacy Law: An International Perspective* (Oxford University Press, 2014) 158. The German Constitutional Court identified such right, but the right to data protection has not been interpreted as such, O Lynskey, *The foundations of EU data protection law* (Oxford University Press, 2015) 178-180 ; P Hustinx, 'EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation', EDPS 2014, 31-32 available at https://edps.europa.eu/sites/edp/files/publication/14-09-15_article_eui_en.pdf p31

[24] Notably, Case 131/12, *Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* [2014] 3 CMLR 50; Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others* [2014] ECR I-238

[25] Hustinx (n 23); N Purtova, 'Default entitlements in personal data in the proposed Regulation: Informational self-determination off the table… and back on again?' (2014) 30(1) *Computer Law & Security Review* 6-24, 12; Lynskey (n23) 180; M Birnhack, 'Review: A Quest for a Theory of Privacy: Context and Control' (2011) 51 Jurimetrics, 447.

[26] M Veale, R. Binns, and J. Ausloos. 2018. "When Data Protection by Design and Data Subject Rights Clash." International Data Privacy Law 8 (2): 121, 105–123; B.J. Koops, 'The trouble with European data protection law' (2014) *International data privacy law*, 4(4) 250-261, 251-253.

[27] One of the possible solutions for resolving these problems would be to create a property-type right over data. However, instituting property rights over data comes with its own concerns. See I Stepanov. 2020. 'Introducing a property right over data in the EU: the data producer's right – an evaluation', *International Review of Law, Computers & Technology*, 34(1) 65-86; Andanda, P. 2019 Towards a Paradigm Shift in Governing Data Access and Related Intellectual Property Rights in Big Data and Health-Related Research. *IIC* 50, 1052–1081; the argument is power that stems from aggregated data should be returned to individuals through the legal mechanism of trusts See Sylvie Delacroix, Neil D Lawrence, Bottom-up data Trusts: disturbing the 'one size fits all' approach to data governance, *International Data Privacy Law*, , ipz014, https://doi.org/10.1093/idpl/ipz014

[28] Lynskey (n23) 254-255, 258-59 under the Directive and in anticipation of the GDPR. Article 29 WP also referred to the 'architecture of accountability' to describe the data controllers' obligations which support data subjects' rights, *Opinion 3/2010 on the principle of accountability*, WP 173, 5

[29] Lynskey (n20)179, 255; similarly, Hustinx (n23); Purtova (n25); Lazaro, C. and Metayer, D.L., 'Control over personal data: true remedy or fairy tale?' (2015) 12(1) SCRIPTed, 12, 18

[30] European Commission, ', EU Commission, *Impact assessment accompanying the document Regulation of the European Parliament and the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation),* SEC (2012) 72, 25 January 2012; Hustinx (n23)

[31] De Hert and Gutwirth in Lynskey (n23) 213 fn 156; Purtova (n25) 7.

responsibility for each participant in the data protection framework if 'the processing of personal data [is] to [truly] serve mankind' as Recital 4 GDPR enjoins.[32] However behind and despite the Directive's and the GDPR's expressed objective to empower data subjects in controlling their data,[33] lies an architecture that implicitly considers all participants in the data protection framework as custodians, directly or indirectly, of the data subjects' data. In particular, the CJEU in *Google Spain* has indicated that the broad definition of data controller includes all entities with factual influence or decision-making powers in order 'to ensure […] effective and complete protection of data subject'.[34] This definition implicitly means that the decision-making process has the potential to create significant asymmetries of power between controllers and data subjects and that there is a need for the controller not to lose sight of its overarching responsibilities to protect data subjects. In effect, we argue that the CJEU describes the controller as a 'custodian'.

We propose the expression 'architecture of custody', instead of 'architecture of control' to convey these notions of balance and shared safekeeping. It better portrays how the data sharing responsibilities in the GDPR and more subtly in the Directive are interwoven between controllers, processors, and individuals, under the supervision of the data protection authorities. We agree with the UK Government's view on 'high standards of data protection law' in the UK[35] while proposing to remedy the serious weaknesses in implementation and enforcement noticed by the Joint Committee on Human Rights in its review of '*The Right to privacy and the Digital Revolution'*[36]. The expression 'architecture of custody' allows us to provide directions for simultaneously improving individual compliance and developing a more pro-active approach to the custody of personal (health) data, feeding within the broader debate on the need for a 'duty of care'.[37]

In order to demonstrate the benefits of this approach, we first present the duties of the controllers and processors when processing data. These principles of custody are then analysed in the context of the DeepMind project to outline the shortcomings in the use of Streams in direct care. We then propose to bring new insights into the drawbacks of the current approach and how our proposal would benefit better data governance in the health care sector and more widely.

2. Principles of custody: initial decisions in processing health data

Data controllers' initial decisions to process health data are subject to several stringent requirements. Because processing health data is in principle prohibited, controllers should strictly justify the processing, and have to undertake data protection impact assessments (DPIAs) when the processing is on a large scale, for example, when hospitals process their patients' health data. Primary custodians of data, controllers may delegate some of the processing to data processors. With the GDPR, the latter are now auxiliary custodians, with specific responsibilities.

[32] Recital 2 Directive 1995/46/EC: 'whereas data-processing systems are designed to serve man'
[33] Recital 7 GDPR; more implicitly, from Recitals 2 and 8, Articles 10-12 Directive 1995/46/EC
[34] Google Spain para 34; Brendan Van Alsenoy, Data Protection Law in the EU: Roles, Responsibilities and Liability, KU Leuven Centre for IT & IP Law Series (Book 6), Intersentia, 2019 p 51, para 81 fn 167.
[35] Department for Digital, Culture, Media & Sport, Online Harms White Paper, Available at https://www.gov.uk/government/consultations/online-harms-white-paper
[36] Report (n19) 31-32
[37] Report (n19) 37; Department for Digital, Culture, Media & Sport, Online Harms White Paper, Available at https://www.gov.uk/government/consultations/online-harms-white-paper; W Perrin and L Woods, Reducing harm in social media through a duty of care, May 8, 2018 available at: https://www.carnegieuktrust.org.uk/blog/reducing-harm-social-media-duty-care/ Accessed 1st February 2020

2.1 The general prohibition to process health data

Data protection laws apply when personal data, i.e. 'any information relating to an identified or identifiable natural person', are being processed.[38] Patients' information is inherently personal data.[39] Their medical records constitute health data, i.e. a 'special category' of personal data,[40] often called 'sensitive personal data'.[41] Health data is distinguished from genetic and biometric data,[42] as any data 'which reveal information about [the data subject's] health status',[43] about the data subject's 'physical or mental health or condition'[44], and is thus not limited to 'ill-health'.[45] The data can be generated in a direct care setting or through apps targeting individuals' well-being, 'irrespective of whether the devices are considered as medical devices'.[46] Medical devices have their own set of regulations both under EU law and UK law, but when personal data is processed, they must also comply with data protection laws. [47]

The GDPR's objective, as well as the Directive's, is to avoid unduly restricting or prohibiting the 'free movement of personal data'.[48] Consequently, processing personal data is permissible per se. By contrast, processing sensitive personal data is in principle, prohibited under the GDPR as it was under the DPA 1998 and the Directive.[49] If undertaken, the processing remains an exception, to be interpreted restrictively.[50] This prohibition stems from the need to specifically protect data subjects against the 'significant risks to a person's fundamental rights and freedoms' such as privacy and discrimination, that the processing of sensitive personal data can bring. [51] The prohibition has a wide scope, in that the processing comprises the collection and all the further uses of the data, including the process of anonymising

[38] Article 4(1) GDPR. Compared to the Directive -Article 2(a)-, the DPA 1998 had a restrictive definition of personal data, leading to an underenforcement of data protection law in the UK. On the variations in transposition, EU Commission (n 27) 14-15.
[39] *Campbell v Mirror Group newspapers* [2004] UKHL 22 [145] per Lady Hale; *R (on the application of W, X, Y and Z) v Secretary of State for Health and Secretary of State for the Home Department, the British Medical Association* [2015] EWCA Civ. 1034 [40].
[40] Article 9 GDPR; Article 8 Directive
[41] Section 2 DPA 1998
[42] Articles 4(13) and (14) GDPR. Under the GDPR, but not under the Directive, these two types of data are sensitive data (Article 9 GDPR).
[43] Article 4(15) GDPR. Recital 35 lists examples of health data. The Directive and the DPA 1998 did not define 'health data', but Article 29 WP did in 'Letter to the Director of Sustainable and Secure Society Directorate of the European Commission,' published 5 February 2015 available online at http://ec.europa.eu/justice/dataprotection/article-29/documentation/other-document/files/2015/20150205_1etter_art29wp_ec_health_data_after_plenary en. pdf and Annex I, p2 at http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2015/20150205letter_art29wp_ec_health_data_after_plenary annex_en.pdf.
[44] Article 2(e) DPA 1998
[45] Article 29 WP (n 43) 2. See also N Purtova, 'Health data for common good: defining the boundaries and social dilemmas of data commons.' In S Adams, N Purtova, and R Leenes (eds) *Under Observation: The Interplay Between eHealth and Surveillance* (Springer, 2017) 177, 190-191
[46] Article 29 WP (n 43) 2
[47] For the details and the links to the UK regulatory authority, see the guidance at https://www.gov.uk/guidance/regulating-medical-devices-in-the-event-of-a-no-deal-scenario
[48] Article 1(3) GDPR; Article 1(1) Directive; the DPA 1998 did not reproduce Article 1(1) Directive, see Bygrave (n23) 117-120; Lynskey (n 23) chapter 3.
[49] Article 9(1) GDPR, former Article 8(1) Directive transposed in Schedule 3(1) DPA 1998.
[50] Article 29 WP, WP 131 (n 18) 11
[51] Recital 51 GDPR; ICO Guide to the General Data Protection Regulation, at https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/special-category-data/; similarly Recital 33 Directive and previous ICO guidance.

personal data.[52] Viewed in this light, even the continuous collection of health data for a medical record and the sharing within the medical team in direct care, so fundamental to the healthcare sector, is on principle prohibited unless the collection and the sharing can be justified and meet the specific requirements set out in the law.

By contrast, ethical guidance and the law of confidence in direct care consider that the collection and sharing of health data within the medical team are per se permitted until, and unless, the patient objects to the recording and/or sharing of the information. The prohibition to use health data is re-instated as a principle only in indirect care after health professionals have collected health data, created medical records and shared them within the medical team for direct care. This shift in perspective between data protection law, on the one hand, and ethical guidance and the law of confidence, on the other hand, means that the balance of rights inherent to Article 1 GDPR and Directive can be said to be tilted towards the individuals' protection of their sensitive personal data, against the data controllers' interests in processing the data.

2.2 Justifying the exception: the requirements for processing health data

The processing of health data builds on the processing of non-sensitive personal data. Already, the latter processing brings two sets of important conditions. Firstly, to ensure its proportionality to the objective underlying the processing, the processing must satisfy the eight principles listed in Article 5 GDPR, former Article 6 Directive, Schedule 1 DPA 1998. Not specific to sensitive data, they are notably that: the processing must be fair and lawful,[53] the GDPR expressly adding transparency; for specific and explicit purposes ('purpose limitation')[54]; and no more and no longer than necessary (data minimisation and storage limitation).[55] Besides, the controller must demonstrate compliance and is thus accountable for the processing, an underlying principle under the Directive which the GDPR rendered explicitly.[56] Secondly, data controllers must justify the processing by choosing the conditions or grounds for lawful processing. Two sets of grounds exist, those generic to all personal data in Article 6 GDPR, former Article 7 Directive, Schedule 2 DPA 1998; and those specific to sensitive data in Article 9(2) GDPR, former Article 8 Directive, Schedule 1 DPA 1998. For sensitive data, the UK chose to require compliance with both, and not just those of Article 9 GDPR, former Schedule 8 DPA 1998. [57] For health data, there is thus an additional layer of protection.

For both personal and sensitive data, consent is the first ground listed for controllers to justify the processing; however, it is not the first or preferred legal basis for data

[52] Article 4(2) GDPR; Article 2(b) Directive;s1(1) DPA 1998. Article 29 WP, *Opinion 03/2013 on purpose limitation*, WP 203, 4.
[53] Article 5(1)(a) GDPR; Article 6(1)(a) Directive; Schedule 1(1) DPA 1998
[54] Article 5(1)(b) GDPR; Article 6(1)(b) Directive; Schedule 1(2) DPA 1998
[55] Article 5(1)(c) GDPR; Article 6(1)(c) Directive; Schedule 1(3) DPA 1998
[56] Article 5(2) GDPR; Article 6(2) Directive; S4(4) DPA 1998
[57] The Directive and the GDPR do not specify. Article 29 WP indicated that both grounds might be necessary, Article 29 WP, *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC*, WP 217, 15. In the UK, Schedule 1 part 1(1)(b) DPA 1998 required both; the DPA 2018 is silent, but the ICO has explained that both Article 6 GDPR and Article 9 GDPR must be satisfied. At https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/special-category-data/.

processing.[58] It is on 'equal footing with the other legal bases' data controller can choose from, both for personal data and sensitive personal data. [59] If free, specific, informed, and unambiguous consent[60] is difficult to obtain, data protection consent should be abandoned.[61] Data protection laws implicitly acknowledge this for health data under Article 9 GDPR, former Article 8 Directive, Schedule 3 DPA 1998. In direct care situations, two other -primary- grounds are available: that of Article 9(2)(c) GDPR, former Article 8(2)(c) Directive, Schedule 3(3) DPA 1998, for emergency treatment, when 'processing is necessary for the vital interests of the data subject'; and that of Article 9(2)(h) GDPR, former Article 8(3) Directive, Schedule 3(8) DPA 1998, for non-life threatening situations,[62] when the processing is necessary to preventive medicine, diagnostic and treatment. The processing under Article 9(2)(h) GDPR cannot extend to other activities such as research or auditing hospitals, even if useful.[63] These are part of indirect care and fall under Article 9(2)(i) or (j). In other words, Article 9 GDPR mirrors the traditional distinction between emergency care, direct care, and indirect care, which is at the heart of ethical guidance and the law of confidentiality, beyond the field of data protection laws.

Regarding Article 6 GDPR grounds, when processing health data, Article 6(1)(d) GDPR, previously Article 7 Directive, Schedule 2(4) DPA 1998, should apply in emergency care situations.[64] For all other aspects of direct care, two grounds seem available: Article 6(1)(e) GDPR, former Schedule 2(5)(b) DPA 1998, when processing is necessary for 'a task carried out in the public interest or the exercise of official authority vested in the controller'; and Article 6(1)(c) GDPR, formerly Schedule 2(3) DPA 1998, when the processing is necessary for the compliance with a legal obligation. These two grounds are incredibly close to each other, but they differ in scope.[65] Article 6(1)(c) GDPR integrates a legal duty to process data as the core function. In contrast, Article 6(1)(e) GDPR covers situations where the controller itself has an official authority or a public interest task, but not necessarily a legal obligation to process data, even though the processing can be necessary for exercising the authority or performing the task.[66] In healthcare, the NHS has a legal duty to provide treatment, but not to process data, despite processing health records being essential to providing treatment. Thus, Article 6(1)(e) GDPR should apply.

Compliance with these requirements under Articles 5, 6 and 9 GDPR, and their equivalent under the Directive and the DPA 1998, is linked to a transparency obligation for controllers towards data subjects. Under Article 10 Directive and Schedule 1 Part 2, para 2(3) DPA 1998, this obligation was centred on informing about the purposes of the processing and any further information 'necessary' for the

[58] Article 29 WP, *Opinion 15/2011 on the definition of consent*, WP 187, 7-8.
[59] Lynskey (n 23) 186.
[60] Article 4(11) GDPR
[61] WP 131 (n 18) 8-9; WP 187 (n 58) 6-7; Article 29WP, *Guidelines on consent under Regulation 2016/679*, WP 259 (2018) 23; ICO Guide to the GDPR, Consent, at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/
[62] WP 131 (n 18) 9-10; ICO, Guide to GDPR (n 57)
[63] WP 259 (n 61) 8, 11; Article 29 WP, *Advice paper on special categories of data ("sensitive data")* , April 2011, 10-11 at http://ec.europa.eu/justice/article-29/documentation/other-document/index_en.htm#maincontentSec7. Complementing the GDPR, the DPA 2018 ends the confusion introduced in Schedule 3(8) DPA 1998, which added medical research (indirect care) in the definition of direct care.
[64] In November 2019, the ICO confirmed that for emergency care, the two grounds correspond, *Guidance on Special Categories of Data* version 1.0.40, p16-17 'How does this affect our lawful basis?'
[65] WP 217 (n 57) 19.
[66] WP 217 (n 57) 19, 21.

processing to be fair, as per Article 6(1)(a) Directive, Schedule 1 DPA 1998.[67] In practice, privacy policies -where present- remained poorly drafted, complex, often difficult to access, and/or confusing with the terms and conditions of a contract.[68] Thus, Article 12(1) GDPR specified the format and Articles 13 and 14 GDPR the type of information needed, mirroring each requirement under Articles 5, 6, and, for health data, Article 9 GDPR, except for the security obligation where information does not have to be provided. Privacy policies can still be multi-layered but should be clearly distinguished from contractual terms[69] and data protection impact assessments,[70] and easily accessible, not 'several clicks' away in 'nested pages'.[71] 'User-centric',[72] the transparency obligation under the GDPR requires controllers to be pro-active, a change from the more relaxed approach under the Directive.[73] Having a website with a privacy notice, but without taking active steps to ensure data subjects actually read the information, does not anymore fulfil the controller's obligation.

Furthermore, compliance with these requirements under Articles 5, 6 and 9 GDPR, and their equivalent under the Directive and the DPA 1998, cannot be an afterthought. It must start before the processing of data begins, and must be maintained throughout the time of the processing, to ensure that the processing consistently remains necessary and proportionate, respectful of the data subjects' rights and interests in balance with the data controllers' interests in collecting and using the data. It is part of a wider preoccupation to ensure privacy and security by design. An implicit principle under the Directive, [74] privacy by design was intended to guide good practice but was not a formal requirement. The ICO was one of the first European supervisory authorities to issue guidance, in an attempt to foster a more pro-active, forward-looking, approach to the protection of data, instead of the more relaxed, reactive attitudes many controllers adopted.[75] Article 25 GDPR transformed this good practice into a legal requirement, with the view that data controllers will take their responsibilities more seriously than some may have had so far.[76]

2.3 Additional constraints: data protection impact assessment (DPIA) for large scale processing of health data

Privacy Impact Assessments (PIAs) emerged as a response to implementing Article 20 of the former Directive: national supervisory authorities had to conduct 'prior checks' where the Member States had determined that 'the processing operations

[67] ICO, The Guide to Data Protection, 2013, B1 para 28; see also, para A1 para 23-28. The ICO indicated that fairness requires controllers to inform data subjects of processing they would not expect, for example when data would be disclosed to a different organisation than the controller.
[68] Academic studies abound as to the quality of privacy policies, notably with regard to consent. In the UK, see notably M Borghi, F Ferretti, and S Karapapa, 'Online data processing consent under EU law: a theoretical framework and empirical evidence from the UK' (2013) 21(2) International Journal of Law and Information Technology 109-153.
[69] Article 29 WP, *Guidelines on transparency under Regulation 2016/679*, WP 260 (2018) para 8, 13, 35; ICO GDPR guidance under 'Right t to be informed' at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-be-informed/
[70] Implicitly, Article 35 GDPR.
[71] WP 260 (n 69) para 35-36
[72] WP 260 (n 69) page 5, para 4.
[73] On the need to be pro-active, WP 260 (n 66) para 36
[74] Article 29 WP, *The Future of Privacy, Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data*, WP 168 (2009) 2-3; ICO, *Privacy by design* (2008).
[75] ICO, *Privacy by design* (n74) 2,10, 15
[76] EU Commission (n 30) 80-82.

[was] likely to present specific risks to the rights and freedoms of data subjects. As one of the leading national supervisory authorities which issued guidance on PIAs as early as 2007,[77] The UK ICO recommended PIAs as a tool and process to ensure 'privacy by design'. The aim was to encourage data controllers: to 'look at the broader issues' a project raises from a privacy point of view; to engage with all stakeholders 'even those who are expected to oppose a particular project',[78] and to minimise risks through the modification of the design before the project starts. [79]

Data controllers could notably involve data subjects in the design of a project or part of a project.[80] The choice of individuals had to be representative, so that 'those likely to be affected ha[d] a voice',[81] 'a meaningful impact'. However, not consulting individuals did not violate the law. The ICO was particularly mindful of security or commercial sensitivity which may play against an organisation revealing 'all of their plans to the outside world'.[82] What mattered was for controllers to identify 'privacy risks, compliance risks and any related risks for the organisation' such as 'fines' and 'reputational damage leading to loss of business.'[83] While not formally required under the Directive and the DPA 1998, the lack of PIAs could lead to a breach of the controller's duties to process data transparently and securely.[84] Under Article 35 GDPR, this good practice has become a stand-alone requirement when the processing 'is likely to result in a high risk to the rights and freedoms of natural persons', notably when 'a large scale of special categories of data […] as per Article 9(1)', unless an impact assessment has already been carried out because data controllers chose Article 6(1)(c) or (e) GDPR as grounds for processing. Large scale processing of health data does not include the processing by individual doctors but does include that by a hospital, including when the processing is routine and inherent to the functioning of the hospital.[85]

The GDPR also refocuses the impact assessments on data protection, rather than solely on privacy, to enlarge the scope of the risks assessment to other rights than the right to privacy. Maybe more clearly than before, the ICO now distinguishes between compliance risks, when an organisation fails to comply with the GDPR, and other, broader, risks to the rights and freedoms of individuals and which can exist even if an organisation processes data proportionately.[86] Building on existing practice, the GDPR strongly recommends that controllers, 'where appropriate', consult 'data subjects or their representatives on the intended processing'. The consultation does not have to be on all elements of the project; and since the

[77] R Clarke, 'Privacy impact assessment: Its origins and development' (2009) 25(2) *Computer law & security review* 123
[78] ICO 2007, *Privacy Impact Assessment Handbook v2.0*, 3-4.
[79] D Wright, 'The state of the art in privacy impact assessment' (2012) 28(1) *Computer law & security review* 54, 55.
[80] ICO, *Conducting privacy impact assessments code of practice*, 2014, 18-19; ICO 2007 (n 74) 28
[81] ICO 2014 (n 80) 19.
[82] ICO 2007 (n 78) 8.
[83] ICO 2014 (n 80) 23, chapter 6.
[84] ICO decision on Royal Free (n 11) principle 1 for transparency, Principle 7, Schedule 1 DPA 1998, for security
[85] ICO guidance 'What does 'large scale' mean? At https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/when-do-we-need-to-do-a-dpia/#when12 ; [85] *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether the processing is "likely to result in a high risk" for the purposes of Regulation 2016/679*, WP 248 (2017) 10
[86] At https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/

exercise is not about obtaining their consent,[87] their views can be discarded as long as data controllers document their reasons to do so. [88] Furthermore, Article 35(9) GDPR allows data controllers not to consult when 'commercial or public interests or the security of processing operations' need protecting, for example, when, in the words of Article 29 WP, the consultation 'would compromise the confidentiality of companies' business plans or would be disproportionate or impracticable'.[89] The only obligation is then to explain why they chose not to consult. Publication of DPIAs is also not an obligation.

Overall, controllers should not lose focus of the rights-based approach inherent to the GDPR and former Directive.[90] Low-risk processing does not exempt controllers from compliance. Instead, risks assessment represents a 'scalable and proportionate approach to compliance',[91] so that the processing respects the balance of rights and interests as per Article 1 GDPR and Directive. A dynamic instrument, a DPIA should be reviewed regularly, and when changes in risks may occur.[92] Furthermore, while compliance falls on controllers, the GDPR has created a duty for processors to assist the controller in fulfilling its obligation under Article 35 GDPR. Processors have become auxiliary custodians.

2.4 Towards processors as auxiliary custodians

Compliance with the above requirements falls primarily on controllers, defined before and with the GDPR, as those who 'determine[…] the purposes and means of the processing of personal data'.[93] While the Directive and the DPA 1998 acknowledged that controllers or joint-controllers could ask others to process 'on [their] behalf', they did not define in great details the relationship between the two. The only obligation established in the Directive and DPA 1998 was for controllers to have a contract with the processor(s) to ensure compliance with the controllers' security obligation.[94] Beyond this, processors' responsibility centred on complying with what the controllers told them to do. The ICO went as far as to state that generally 'data processors are not directly subject to the Act'.[95]

The GDPR brought in that respect 'significant' changes, as the ICO has underlined in its initial GDPR guidance for those established in the UK.[96] Article 28 GDPR obliges processors to assist controllers, not just in fulfilling their security obligations, but also in the recording of processing activities for accountability purposes, in the notification of data breaches and the conduct of data protection impact assessments. Contracts are obligatory and in writing, including in electronic form, and processors 'shall immediately inform the controller if, in its opinion, an instruction [from the controller] infringes' Article 28 GDPR.[97] Processors must thus be vigilant and not passive

[87] WP 248 (n 85) 15.
[88] WP 248 (n 85) 15; ICO (n 57)
[89] WP 248 (n 82) 15; ICO (n 57) 'step 3'
[90] Article 29 WP, *Statement on the role of a risk-based approach in data protection legal frameworks*, WP 218 (2014) 3
[91] Article 29 WP (n 90) 2
[92] Article 35(11) GDPR
[93] Article 4(7) GDPR; Article 2(d) Directive, Article 1(1) DPA 1998
[94] Article 21 Directive; Schedule 1(Part II) DPA 1998
[95] ICO (n 67) A3 para 26
[96] at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/controllers-and-processors/what-s-new-under-the-gdpr/#1
[97] Article 28(3) GDPR

concerning controllers' decisions. They have become auxiliary custodians of individuals' data in the eye of the law, without reducing the respective responsibility of controllers.

3. Implications for the processing in the operational use of Streams

In Streams, the Trusts decided to process and allow DeepMind to process health data. As such, they can be considered as data controllers and DeepMind, now Google Health UK, as a data processor. For this article, we do not question this sharing of responsibilities and whether they are or not joint controllers.[98] Whether or not DeepMind is a controller does not change the fact that the Trusts would, in both instances, remain primary custodians. Therefore, we focus on articulating whether the Trusts fulfilled their obligations as primary custodians and DeepMind as auxiliary custodian. After an outline of their obligations in Streams, we demonstrate their shortcomings in ensuring the lawfulness of the processing as much as its proportionality.

3.1 The shortcomings in ensuring the lawfulness of the processing

The Streams app, when used in direct care, i.e. in a clinical setting, processes different data sets: the health data that the Trusts hold on their patients, and the personal data of the health care professionals using the app to authenticate themselves. The latter data set, barely mentioned in the documentation on Streams,[99] is unlikely to involve sensitive personal data; its processing is thus unlikely to be prohibited per se, although it still has to comply with data protection requirements. By contrast, the Trusts' patients' health data –which is the sole focus of this paper- is subject to the original prohibition of processing health data in data protection law. The Trusts need to treat the processing as an exception rather than the rule, even if ethical guidance for direct care presumes the opposite. That the Streams app has also been approved as a medical device[100] Does not exonerate the Trusts from complying with data protection requirements. They will have to identify, according to the situations of direct care considered, the following justifying grounds: Article 9(2)(c) or (h) GDPR; and Article 6(1)(d) or Article 6(1)(e) GDPR.

Royal Free has put forward the 'vital interests' of its patients under Article 6(1)(d) GDPR, former Schedule 2(4) DPA 1998, but not under Article 9(2)(c) GDPR, former 3(8) DPA 1998.[101] It relies solely on Article 9(2)(h), which is inaccurate for emergency care situations. RF is thus only partially compliant with the GDPR and previously with the DPA 1998. The Linklaters' auditing analysis is also questionable as they do not identify Article 9(2)(c) GDPR despite identifying Article 6(1)(d) GDPR.[102] Consequently, for the ICO to conclude that it is satisfied with RF's compliance with the GDPR is surprising. The other three Trusts do not refer to the

[98] Powles and Hodson (n 5)
[99] And certainly, with no analysis of potential risks for the hospital staff whose details are processed.
[100] After Royal Free initially failed to engage with this specific regulatory process, Powles and Hodson (n 5
[101] PIA v0.3 at http://s3-eu-west-1.amazonaws.com/files.royalfree.nhs.uk/AboutUs/Privacy_Impact_Assessment_Streams_Barnet_Extension.pdf; also identified by the auditing firm Linklaters, Linklaters Report, *Audit of the acute kidney injury detection system known as Streams The Royal Free London NHS Foundation Trust*, [May 2018], 43, para 23.2 at https://s3-eu-west-1.amazonaws.com/files.royalfree.nhs.uk/Reporting/Streams_Report.pdf
[102] Report (n 101)

emergency care ground of Articles 6 and 9 GDPR, even when they expressly indicate, as Taunton and Yeovil do, that the app will be used for patients in emergency care.[103] The processing is thus not lawful in this situation.

In other situations of direct care, the Trusts should be able to rely on Article 9(2)(h) GDPR and should clearly distinguish clinical use (direct care) from the testing and piloting of the app (indirect care), as the latter cannot be justified under Article 9(2)(h) GDPR. Before the GDPR, Schedule 3(8) DPA 1998 referred to both direct care and research, introducing doubt as to whether research should be conducted under Article 33 DPA 1998 transposing Article 8(4) Directive which justified research, or under Schedule 3(8) DPA 1998 which transposed Article 8(3) Directive but where the Directive focused solely on direct care. The GDPR eliminated any possible confusion: Article 9(2)(h) concerns direct care and must be distinguished from Article 9(2)(j) applicable to research.

The problem in Streams is that the DPIAs -where the hospitals specified the grounds- do not always distinguish between the clinical use and the testing of the app. They often refer to both uses, without mentioning a ground other than that of direct care, even though the analysis would be different since the necessity to conduct research does not equate to the necessity to process data for treatment. For Yeovil and Taunton, it is only retrospectively because the Trusts indicated they stopped the processing before the app went live- that the processing seems to have been done for testing purposes only, not direct care purposes.[104] While the Trusts might have been confused by the wording of Schedule 3(8) DPA 1998, the enactment of the GDPR in April 2016 left no doubt as to which ground would become applicable. Article 9(2)(h) GDPR cannot apply to the testing of the app. The Trusts should have distinguished more clearly. In contrast to the Trusts' DPIAs, the audit report on Royal Free clearly distinguished between testing and clinical use, but like the Trusts, the report justified the testing of the app under Article 9(2)(h) GDPR.[105] That the ICO did not rectify Linklaters' unsustainable use of Article 9(2)(h), GDPR is problematic. Complying with Article 9(2)(h) GDPR requires that health professionals, for which s204 DPA 2018 provides a list, and anybody working under their responsibility, are subject to an obligation of secrecy, interpreted as the duty of confidentiality.[106] The Trusts' personnel is obviously under an obligation of confidentiality, as well as DeepMind.[107] The processing is in that respect lawful.

---

[103] Yeovil (n 14) and at https://www.yeovilhospital.co.uk/wp-content/uploads/2017/11/PRIVACY-IMPACT-ASSESSMENT.pdf; for Taunton at https://www.tsft.nhs.uk/media/513512/deepmind-pia-2-nov-2017-final.pdf'

[104] See n 14 & 16

[105] Linklaters Report (n 101) 1, para 1.2. Schedule 3(8) DPA 1998 for direct care also mentioned research, but was probably violating the Directive as medical research was under Article 8(4) Directive, i.e. s33 DPA 1998. Article 29 WP clearly excluded medical research from Article 8(3) Directive, WP 131 (n 18) 10. If any doubt subsisted under the DPA 1998, they disappeared with the GDPR.

[106] Article 9(2)(h) GDPR and Article 9(3) GDPR; s10(1)(c) DPA 2018; Article 8(3) Directive and Schedule 3(8) DPA 1998.

[107] See The service agreements are on DeepMind's website at https://deepmind.com/applied/deepmindhealth/transparency-independent-reviewers/ available at http://s3-eu-west-1.amazonaws.com/files.royalfree.nhs.uk/Privacy_Impact_Assessment___Streams___Royal_Free_Hospital.pdf Yeovil District Hospital NHS Foundation Trust (Yeovil), at https://deepmind.com/blog/bringing-streams-yeovildistrict-hospital-nhs-foundation-trust/ and at https://yeovilhospital.co.uk/new-mobile-app-will-improve-patientcare/;Taunton and Somerset NHS Foundation Trust (Taunton), at https://www.tsft.nhs.uk/patients-andvisitors/confidentiality-and-data-protection/; Imperial College Healthcare NHS Trust (Imperial College) at https://www.digitalhealth.net/2019/01/imperial-deepminds-streams-app/ and the roll out was announced on 21 January 2019, see https://www.imperial.nhs.uk/about-us/news/new-technology-partnership-to-help-patient-safetyand-care

More importantly, Article 9(2)(h) GDPR, former Article 8(3) Directive, Schedule 3(8) DPA 1998, requires demonstrating that the processing is necessary for direct care. Necessity does not mean the processing has to be 'absolutely essential'. It has, however, to be 'more than useful',[108] beneficial or 'standard practice'[109]. If the same purpose can be fulfilled by other 'less intrusive means', then the processing is not necessary to direct care.[110] In that respect, Linklaters' reference to 'reasonably necessary', a lower threshold to that of 'strictly necessary', [111] violates the ICO's clear guidance available under the DPA 1998 and the GDPR.[112] While the ICO expressly states that it does not condone the report, its silence can be misinterpreted as acceptance of the audit's interpretation, notably when the ICO indicated that, for another area of law, the report was mistaken in its interpretation.

In order to demonstrate necessity, all Trusts put forward the benefits of Streams, i.e. its ability to improve the diagnostic of AKI but vary in their degree of details. Imperial College presents no other elements than the generic benefits of Streams and thus is unlikely to meet its requirements. Taunton and Yeovil explicitly state that without Streams, clinicians have to log into different IT systems simultaneously in order to see all the information needed to diagnose AKI. Yeovil's assessment of necessity seems reinforced by its rejection of opts-out, on the basis that they are unsafe and unpractical, as the Trust would have to maintain two different systems according to which patient rejected or accepted the use of Streams.[113] However, Taunton, with whom Yeovil works and shares patients' health data under the existing system OrderComms,[114] allows for opt-outs, like Royal Free. Does it mean that Streams, while beneficial and improvement, is not strictly needed?

It could reasonably be argued that while the old system could still be used (as in Taunton), Streams brings enough significant improvement to be 'more than useful or beneficial' and thus to be strictly necessary for direct care. In that sense, Royal Free mentions that clinicians can view two sets of results together rather than separately.[115] Linklaters also recommends that Royal Free clearly explained the negative consequences on its patients' care when they opt-out, which implies that the clinical use of Streams may not be absolutely essential but remains significant enough to be necessary for providing good quality care. Therefore, the Trusts could be justified in their use of Article 9(2)(h) GDPR. Royal Free's, Taunton's and Yeovil's assessments on necessity may be sufficiently detailed to demonstrate compliance, which is an express requirement under Article 5(2) GDPR. They are, however, undermined by their contradiction in offering or rejecting patients an opt-out. That Taunton and Yeovil ultimately decided not to use Streams for clinical care also raises questions as to whether the Trusts decided so because they could not justify the necessity of the processing or because other reasons underlined their decisions. For Imperial College, its failure to articulate necessity beyond the generic benefits of Streams is likely to constitute a violation of Article 5(1)(a) GDPR, former Schedule 1

[108] WP 131 (n 18) 10; ICO (n 67) B3 para12-15
[109] ICO Guide on the GDPR (n 57)
[110] ICO Guide on the GDPR (n 57)
[111] Report (n 101) para 22.8.
[112] ICO (n 67) B9, para 14
[113] Yeovil PIA (n 103) 4.
[114] Yeovil is silent on this connection, PIA (n 103); Taunton is explicit, PIA (n 103) 1
[115] PIA v0.3 (n 101) and PIA v0.1 at http://s3-eu-west-1.amazonaws.com/files.royalfree.nhs.uk/Privacy_Impact_Assessment___Streams___Royal_Free_Hospital.pdf

DPA 1998, unless it can bring other (unknown) documents to demonstrate it had articulated the processing's necessity under Article 9(2)(h) GDPR.

Compliance with Article 9(2)(h) GDPR does not suffice. The Trusts must also justify the processing under Article 6 GDPR, former Schedule 2 DPA. Yeovil and Taunton have agreed on Schedule 2(5)(b) DPA 1998, now Article 6(1)(e) GDPR. Although Royal Free does not state another ground that emergency care, Linklaters proposed the same analysis as Taunton and Yeovil for Royal Free, by reference to the NHS trusts' statutory function to provide healthcare under s43 NHS Act 2006.[116] Imperial College uses, however, Article 6(1)(c) GDPR by reference to s25 NHS Act 2006, which gives the Secretary of State power to establish NHS Trusts. Article 6(1)(e) Directive is likely to be the correct ground as the legal obligation of the NHS is not to process data but to provide treatment.[117] Imperial College should thus use the same ground as Yeovil and Taunton. Its reference to s25 NHS is not material, in our view, as it mentions the function of the NHS - providing healthcare- as s43 does. Royal Free should also adopt and specify this ground in its future documentation and avoid the silence of its current DPIAs.

To summarise, the Trusts do not fully comply with Article 5(1)(a) GDPR. For emergency care, all Trusts failed to identify Article 9(2)(c) GDPR, and Royal Free is the only one having identified Article 6(1)(d) GDPR. All Trusts identified Article 9(2)(h) GDPR for the processing, but none is particularly evident as to whether the processing concerns the clinical use of the app or the testing of the app. For the latter, Article 9(2)(h) is inapplicable. Besides, Imperial College still violated its obligations by not demonstrating the necessity of the processing. Unfortunately, the Trusts' shortcomings do not stop here.

3.2 *The shortcomings in ensuring the proportionality of purposes, data and timing of the processing*

Under former Article 6(1)(b) Directive, Schedule 1 DPA 1998, as under Article 5(1)(b) GDPR, a 'general purpose' or 'umbrella purpose' is not acceptable. The requirement is here intrinsically linked to the controllers' obligation of transparency now expressly part of Article 5(1)(a) GDPR. A generic purpose should be followed by specific (sub) purposes to be listed, if not in the first layer of documents, at least in a more detailed one.[118] The DPIAs state that Streams helps managing AKI and benefits patients, and that DM will not process the data for other purposes than those stated and that it will not use artificial intelligence, machine learning or unauthorised algorithms. Beyond that, details are scarce. Yeovil considers Streams no more different than other IT systems it uses; an argument also put forward for Royal Free in the Linklaters' report. [119] The argument misrepresents the purposes. Streams' function is not to passively keep patients' health records which clinicians later consult to assess risks of AKI. It provides algorithmic assistance to clinicians by flagging the risks of AKI. Comparison with other IT systems also masks the specific uses of Streams.

According to Royal Free's dedicated webpage on DeepMind, Streams seems to allow: viewing the clinical records and results, including side-by-side which was not before possible; viewing the outcome of the AKI algorithm and how the outcome was determined; sending an alert to clinicians following the AKI algorithm, and offering a

[116] Report (n 101) Addendum 1
[117] Supra section 2.2
[118] WP 203 (n 52) 6, 13-14, 53; ICO (n 57)
[119] Report (n 101) para 23.2, p43

chat facility to health professionals to discuss the results. Royal Free made this information available except for the chat facility- through its video, easily accessible from its website. [120] On the other hand, the DPIAs, which are supposed to establish specific purposes, remain vague. On balance, Royal Free's information may suffice to comply with its obligation to indicate the purposes. However, Royal Free could do with improving the information in its DPIA documents and avoid the misleading statement that Streams is similar to other IT systems. All the other Trusts fail to comply with their obligation under Article 5(1)(b) GDPR. Promoting the benefits of Streams for managing AKI is not informing. It might suffice as a 'first-layered' approach, but it remains an 'umbrella purpose', to be complemented by more detailed information.

Furthermore, the Trusts must use only the data necessary for the specific purposes identified: no less, no more, and not just because the data is merely useful.[121] Imperial College states that all patients of the Trust are entered but that the app will notify clinicians only the patients who underwent creatinine blood tests.[122] For its patients, Royal Free has never been clear, and it took the ICO 2017 decision to confirm that all patients' data have been used for the testing of the app (indirect care),[123] without change having been noted in the Linklaters' 2018 report concerning clinical use. For the Barnet extension, Royal Free provides no details beyond 'inpatients' and a sweeping statement that '1.97 million records for 1.33 million patients' are processed, without any explanation as to what the difference means.[124] Linklaters noted that some Royal Free's patients might never need Streams; nevertheless, Royal Free was justified in processing all its patients' data because RF cannot predict which patients in the future would need to be assessed for AKI.[125]

This argument may seem in line with the ICO guidance under Schedule 1 DPA 1998 and under the GDPR: 'it is permissible to hold information for a foreseeable event that may never occur' for example when an employer holds its employees' blood groups because of the dangerous nature of the work and the possibility of an accident.[126] However, Royal Free's explanation of necessity relayed by Linklaters seems seriously undermined by Yeovil and Taunton's justification for restricting the nature and volume of data they transfer to DM. While Taunton and Yeovil do not state the number of patients whose data is transferred, both Trusts select data based on 'the clinical applicability and relevance of the data […] utilised for clinical assessment of patients'. These medical criteria may be revisited if the need to use Streams arises for other patients currently 'excluded'. [127] Therefore, serious doubts arise as to whether Royal Free and Imperial College have justified the necessity of processing all their patients' data. As DeepMind does not use machine learning and has merely coded the existing algorithm which the NHS has created, it is difficult to see how the use of all patients' data could be justified. There is no need technically at least to enter a large set of data to identify patterns and correlations which would

[120] At https://www.royalfree.nhs.uk/patients-visitors/how-we-use-patient-information/our-work-with-deepmind/
[121] WP 131 (n 18) 10
[122] SA (n 106), para 21.3.
[123] ICO decision (n 11)
[124] PIA v0.3 (n 101) section 2, question 5.
[125] Report (n 101) 23.2
[126] ICO (n 67), B3, para 14-15; Guide to GDPR guidance on 'data minimisation' (n 57)
[127] Yeovil, PIA (n 103) 5-6; Taunton, PIA (n 103) 7, 9-10

not otherwise be visible.[128] Therefore, it could be argued that those patients who are absolutely not at risk of developing AKI should not have their data entered into Streams. If a patient later develops symptoms that may put them at risk and require the use of the algorithm to assess the risks of developing AKI, their data could then be transferred to Streams and analysed by Streams, as Yeovil and Taunton explained.[129] Therefore, while all hospitals list the various data points for patients,[130] Royal Free and Imperial College have not demonstrated that they comply with the data minimisation principle.

Finally, compliance with the storage limitation principle is problematic.[131] Data should be processed no longer than necessary. The principle notably requires assessing which historical data is needed (the whole medical record; or part of it), and for how long the data will be retained in Streams. If a date cannot be given, the criteria for assessment need to be provided with regular reviews scheduled for re-assessing proportionality. Royal Free, Yeovil and Taunton refer to the clinical assessment needs to justify: for Royal Free, 5 years of medical records, with an increase over time as no removal of data is scheduled;[132] for Yeovil, 5 years for patients within the last 6 months; [133] and for Taunton, an initial 3 months retention period, increased to 3 years. [134] Imperial College provides no timeline, just a reference to 'standard retention policies relating to other ICHNHST clinical systems' and contractual agreements, without any link to other sources which would enlighten the reader. [135] Across the hospitals, there is no indication that the data will be removed because the patient ceases to be in their care or because the patient's recovery has been long enough to justify interrupting the monitoring of the risk to develop AKI. Thus, while patients know that medical criteria are used to retain the data in the app, they are unable to assess the proportionality of the processing period, since no element of comparison, such as the so-called standard NHS retention period, is indicated. Consequently, the Trusts have not demonstrated their compliance with the storage limitation principle.

3.3 The shortcomings in the Trusts' transparency obligations

Each Trust has at least one webpage with a generic privacy policy not specific to Streams. Yeovil has no privacy policy on Streams beyond two (vague) media press releases only accessible through its search engine and which links to the DPIA and the DeepMind website for the contract. The press releases have not been updated to reflect the fact that Yeovil stopped working with DeepMind and did not renew the contract with Google Health UK. Yeovil thus not only violated the DPA 1998 but also violates the GDPR by not keeping its information up to date.[136]

---

[128] On how machine learning creates a challenge to data minimisation for health data, see R Pierce, 'Machine Learning for Diagnosis and Treatment: Gymnastics for the GDPR' (2018) 3 *European Data Protection Law Review*, 333, 342.

[129] Royal Free has included patients' data when under dialysis but does not explain it on its website. On the choice to incorporate it: Linklaters Report (n 101) 15 para 10.5.

[130] All PIAs mention processing of staff's data. RF did not initially state it in its PIA of November 2016 (available as Attachment 5 at https://www.gov.uk/government/publications/request-for-correspondence-between-the-ndg-and-the-royal-free).

[131] Article 5(1)(e) GDPR ; Article 6(1)(e) Directive ; Schedule 1 Part 1(5) DPA 1998

[132] PIA v0.1 (n 115), section 2, question 23; PIA v0.3 (n 101) section 2, question 7.

[133] PIA (n 103) p 5

[134] PIA v3.0 (n 103) at 7

[135] PIA (n 103); id. Royal Free, PIA nov 2016 (n 130) 5

[136] Changes must be notified, WP 260 (n 69) para 39

By contrast, Royal Free has 2 videos on a webpage dedicated to DeepMind, with a 'data protection' section explaining the main general-purpose, the legal grounds for the processing, the retention period, and the patients' rights. The same page links to a short privacy policy for Streams and two DPIAs.[137] The webpage is easily accessible from the main 'how we use your information' webpage under the 'Patients and visitors' tab. Taunton published its 2017 DPIA and its 2018 patient-friendly version, easily accessible on its 'Confidentiality and privacy' webpage.[138] The 2018 document, despite its PIA title, effectively worked as a privacy policy, albeit without stating the legal grounds for processing and the retention period. While such information was easily retrievable in the 2017 DPIA document, the patient-friendly version did not refer to the other document, contrary to what would be expected under a multi-layered approach. In that sense, Taunton did not fully meet its obligation under Articles 6(1)(a) GDPR and Schedule 1 DPA 1998, until it indicated that it has ceased to collaborate with DeepMind.

Imperial College has no dedicated webpage to Streams. In its main privacy policy webpage, it provides three links: one to a PDF document related to Streams, but without saying so before one clicks and reads the document; one to DPIAs as further publications without mentioning Streams; and one link to a press release on Streams accessible through its search engine. The lack of visibility of these documents, the poor quality of the short version not completed by the second layer of information, and the fact that a DPIA is no substitute for a concise and precise privacy policy, means that Imperial College violated the DPA 1998 and violates the GDPR.

To summarise, of the two Trust still using the app, Royal Free is the only one likely to comply with its obligation, whereas Imperial College never did and still does not. Yeovil still violates the GDPR; and Taunton, although more compliant than Yeovil, was not so until it notified the end of the collaboration with DeepMind. The temptation is to praise Royal Free's approach, but Royal Free became compliant only after the ICO concluded it violated the transparency principle under DPA 1998 and obliged Royal Free to sign an undertaking to become compliant and be audited. The Trusts consulted the ICO, but the regulator did not seem to have scrutinised the Trusts as it did for Royal Free. The audit of Royal Free revealed both a serious improvement and some remaining shortcomings by Royal Free not anticipating enough what the GDPR would require in terms of pro-active communication.[139] It is thus quite possible that Royal Free's mindset towards compliance has been heavily influenced by the ICO's negative findings, rather than stemming from an internally-driven change of culture. Furthermore, the fragmentation of the NHS shows the differences between the Trusts in terms of quality of the information provided, ease of access for patients/data subjects, and in the knowledge that we have not investigated whether or not the Trusts took pro-active steps to communicate about the processing.

Nevertheless, the Trusts cannot be accused of systematic lack of transparency, nor DeepMind for that matter. For example, Taunton consulted data subjects, where it was under no obligation to do so under the DPA 1998, thus testifying of its

[137] On the right side, at https://www.royalfree.nhs.uk/patients-visitors/how-we-use-patient-information/our-work-with-deepmind/

[138] With an added link to its more detailed generic privacy webpage. The documents disappeared when Taunton ceased to work with DM (n 103)

[139] Report (n 101) para 25.2 and 25.3

willingness to engage with data subjects and be transparent towards them. [140] Furthermore, the Trusts published some DPIAs, where neither the DPA 1998 nor the GDPR require controllers to do so. In fact, in light of the guidance under both legislations, for which publication is recommended but can be in a summarised form, the apparently unredacted DPIAs can be perceived as the Trusts' willingness to be transparent. Yet, this window on the Trusts' processes also raises questions. Only selected DPIAs were published, without an indication as to why a certain version has been picked and not another, and often without a log of the different versions.[141] If conducting DPIAs serves to demonstrate transparency and accountability of processing, as part of privacy by design,[142] not publishing them raises questions as to how confident data subjects can be that what has been so far published is representative of the steps controllers undertook towards compliance. Furthermore, some DPIAs were published only through Freedom of Information requests. Given the absence of a duty to publish, it would be unfair to conclude the Trusts were unwilling to circulate these DPIAs. However, the situation begs the question as to why the GDPR does not require publication of risks assessment, at least when undertaking DPIAs is compulsory for controllers. Relying on the FOA for DPIAs information, when the Act only applies to public authorities, seems short-sighted.

Similarly, neither the DPA 1998 or the GDPR obliged the Trusts to publish the contracts with DeepMind, and guidance in that respect is simply nil, hence, for the Trusts not to do so on their website cannot be viewed as a failure to follow the good practice or as a violation of a legal requirement. In fact, Yeovil's weblink to DeepMind's website for people to access the contract can even be lauded as a pro-active step towards transparency. For the same reasons, that until recently, DeepMind, as a processor under the control of the Trusts, published the SAs and IPAs can be viewed in a positive light. With DeepMind's absorption into the Google Health Unit in September 2019, this information has simply disappeared from DeepMind's website and Google Health website.[143] Through FOI requests, the new contracts for Taunton and RF have been published, but not yet for Imperial College. [144] How regulators would interpret, this situation is difficult to know. Given Google's history of violations of the transparency requirement both under the Directive and under the GDPR, the change is unlikely to foster a climate of trust in Google's willingness to be forthcoming about its processing. On the other hand, accountability before regulators does not equate to transparency towards the general public, so, the non-publication of contracts (outside FOIs) is unlikely to violate the Trusts' obligations or the processors' obligations under Article 28(3) GDPR, or for transparency under Article 5(1)(a) GDPR, so long as the Trusts can demonstrate compliance before the ICO.

[140] PIA (n 103) 2, 5; PIA (n 103) section 2.3

[141] RF has completed a PIA on 1st September 2017 but never published it. Imperial College's published version is version 4. Taunton's published DPIA version 4.7 is not mentioned under 'media' news but is irretrievable through the Trust's search engine https://www.tsft.nhs.uk/media/540371/Streams-PIA-Version-48-pilot-and-patient-care.pdf

[142] WP 248 (n 85) 14, 18

[143] D King, 'DeepMind's health team joins Google Health', 18 September 2019, at https://deepmind.com/blog/announcements/deepmind-health-joins-google-health, with a link to https://health.google/

[144] Yeovil did not renew its contract (n 15)

3.4 Conclusion

In custody of health data, they are prohibited from processing, and the Trusts must demonstrate the necessity and proportionality of the exceptional processing. The above analysis highlights that there have been patches of compliance, depending on the requirements and the Trust considered. The core issue is the fragmentation of the Trusts' assessment of the necessity and the proportionality of the processing. Even though it is the same app and the same processor, the Trusts differ on: type and volume of data; retention periods which the processing involves; lawful grounds for processing data; and not clearly distinguished between direct care and indirect care, despite data protection laws requiring so. They do not publish the same amount of information and the same type of information, with FOI requests being a critical mechanism for ensuring transparency rather than the data protection laws themselves.

These differences in assessment and approach to transparency can be explained by the NHS being a disjointed organisation, but the argument cannot explain why the ICO, consulted by each Trust during the DPIA process, did not point out their respective contradictions or whether the ICO was in a position to do so. The NHS's fragmentation does not explain either why the ICO stayed silent on the auditing report's misinterpretations of the law and of its own guidance available at the time. We argue that conceptualising data protection as an architecture of custody allows to join the dots and to promote a more pro-active approach to compliance where the controllers' decision-making power ceases to be detached from its objective, i.e. the protection of data subjects, and where ensuring compliance is not just the duty of controllers, but also the duty of others, processors, citizens, and regulators.

4. Conceptualising the architecture of custody: the need for a pro-active approach

GDPR still focuses on control by data subjects instead of custody. DeepMind project highlighted ICO's limited ability to scrutinise the practices of data controllers and its restricted capacity. Data protection law, in an attempt to be technologically neutral, is silent on imposing specific innovation requirements on data controllers[145].

4.1 Changing the primary custodians' approach to data protection

Each Trust seems to have envisaged its compliance in isolation. Imperial College, Taunton and Yeovil drafted their DPIAs after Royal Free started to use Streams for direct care. Given the media attention and the ICO's intervention, the three Trusts knew of Royal Free's processing. However, from the documentation available, they do not seem to have consulted each other and/or to have considered how their isolated approach could result in contradictory assessments of the processing's necessity and proportionality, with the risk of undermining the legitimacy of their respective assessments.

Certainly, no element of the DPA 1998 and the Directive pointed towards adopting a more coordinated approach to data protection for technical products used by different controllers. Guidance on DPIAs did not mention the possibility that several controllers could get involved for similar processing, and processors such as DM had no legal obligation to be pro-active towards the Trusts beyond ensuring data

[145] Veale, Binns, and Ausloos. (n 26)

security. Yet, for the CJEU in *Google Spain*, the Directive's wide definition of a controller exists 'to ensure […] effective and complete protection of data subject'.[146] The controller decides on the processing after having balanced its own rights and interests with data subjects' rights and interests, as per Article 1 of the Directive. Its role as a primary custodian requires a broader outlook of the processing beyond the controller's organisation.

For Streams, it is difficult to argue that the protection of the data subjects is 'effective and complete', to take the words of the CJEU when the Trusts disagree on so many aspects of the processing: the type and volume of data they use for Streams; the retention period they implement; (to a certain extent) the legal grounds; and the rights the data subjects can exercise. We argue that custody stopped at their doorstep. Despite the commonalities of the project, the Trusts have not viewed their individual decision-making power as part of a whole, with a responsibility to take a more holistic approach, so that all patients for whom Streams is used can benefit from equal protection of their data. Even Yeovil and Taunton, which work together, and which may treat the same patient, could not agree on the rights of their patients: Taunton allowed the right to object, but Yeovil banned it. The vocabulary of custody brings to light what the Directive suggests: data processing decisions should not be reduced to a controller's individual control on, and interests in, the processing, but should be envisaged as a means to an end: to protect data subjects within a wider context.

The GDPR, we argue, moves the goal post further, confirming that being a custodian is not about ticking the relevant boxes on a compliance checklist, but about taking a more pro-active and holistic approach to compliance. The transformation of DPIAs from good practice to a legal requirement when the processing involves high risks (profiling, sensitive data, criminal convictions) is a good example. Controllers should use DPIAs to look at a processing's impact on the 'rights and freedoms of natural persons'. This means not only widening the range of rights considered, beyond the right to privacy, to include 'freedom of speech, freedom of thought, freedom of movement, the prohibition of discrimination, right to liberty, conscience and religion'.[147] It also means that DPIAs under the GDPR is 'a tool for managing risks to the rights of the data subjects, and *thus takes their perspective*' in contrast to 'risk management in other fields' which 'focuses on the *organization'*.[148]

Viewing controllers as primary custodians also provide a direction as to what controllers should do when the GDPR itself provides 'get-out clauses' or where Recitals recommend a course of action, but Articles do not create corresponding legal requirements. For example, controllers' duty to consult data subjects or their representatives in the course of a DPIA exists 'where appropriate' and 'without prejudice to the protection of commercial or public interests'.[149] In practice, such consultations -if undertaken- may often constitute nothing more than a form-filling task because controllers have 'economic incentives to minimise obligations' and lose sight of their more general duty to promote data protection by design. [150] To view

[146] Google Spain para 34; Brendan Van Alsenoy, Data Protection Law in the EU: Roles, Responsibilities and Liability, KU Leuven Centre for IT & IP Law Series (Book 6), Intersentia, 2019, p 51, para 81 fn 167.
[147] WP 248 (82) 6, in guidance to Article 35(1) GDPR.
[148] Our emphasis, WP 248 (n 82) 17
[149] Article 35(9) GDPR
[150] Veale, Binns, and Ausloos (n 26) 118, 121; see also R Binns, 'Data Protection Impact Assessments: A Meta Regulatory Approach' (2017) 7 International Data Privacy Law 22

consultations as part of an architecture of custody avoids the trap of invoking commercial interests to protect an organization without first and foremost having truly balanced the organisation's interests with their custodian's duties towards the data subjects and their rights.

For Streams, Recital 92 GDPR is one of the most interesting examples of how interpreting the GDPR as an architecture of custody changes the dynamics of compliance for primary custodians. The Recital, with no previous equivalent in the Directive, states that in some circumstances 'it may be reasonable and economical for the subject of a data protection impact assessment to be broader than a single project, for example where public authorities or bodies intend to establish a common application or processing platform or where several controllers plan to introduce a common application […] across an industry sector […]'. The Recital's suggestions seem to echo Article 35(1) GDPR that '[a] single assessment may address a set of similar processing operations that present similar high risks.' Yet, the GDPR does not provide more details or require the Member States, for example, to establish mechanisms that would limit the diversity of assessments.

In the UK, in the absence of any provision to that effect in the DPA 2018, coordination effectively relies on the willingness of the different controllers to come together. The temptation for controllers is to continue as usual and not to coordinate their DPIAs. The ICO guidance barely mentions the situation, referring to Recital 92 GDPR and the Article 29 WP's guidance but without quoting them, effectively leaving individuals free (not) to check the documents and discover the Recital and the detailed guidance. [151] But if controllers such as the Trusts in the Streams project, consider themselves as primary custodians, 'proxy guardians'[152] of their patients' data *beyond* their individual processing operations and their own organisations, then they are pushed in taking active steps to consult the existing Trusts as per Recital 92.

To summarise, because controllers remain the decision-makers, they should be the primary custodians of data subjects' personal data, undertaking at every stage of the process a balancing exercise between their interests and the data subjects' rights and interests. By increasing their responsibilities, the GDPR reinforces their position as initially envisaged by the Directive, but the fallacy is to 'put too much faith in the controllers' who, faced with complex rules, may choose the path of least resistance 'without understanding much about data *protection*'.[153]

With an architecture of custody in mind, this illusion of compliance can be avoided. Controllers have to interpret their obligations differently, as an exercise in custody rather than a controlling power. As importantly, they should not see themselves as sole and isolated custodians. Other actors in this architecture have a role to play, that of supporting them in their decisions on processing, with the same objective: protecting data subjects.

4.2 Supporting primary custodians and thus data subjects

Recital 7 GDPR leaves no ambiguity: 'Natural persons should have control of their own personal data.' However, control can be an illusion. The Streams project shows the blind spots of the law if one counts solely on data subjects' personal actions to

[151] ICO (n 85)
[152] Munns, C. and Basu, S., *Privacy and Healthcare Data: 'choice of Control 'to' choice' and 'control'*, (Routledge, 2017)
[153] Koops (n 26) 253-255

check on the controllers' decisions on processing. Rather than focusing on control, it would be more judicious to look at other actors' roles to support primary custodians in taking the right decisions.

4.2.1 *The limits of data subjects' control: the recognition of NGOs' right of legal action under Article 80 GDPR*

The initial criticisms of the project stemmed from a journalist who used FOI requests to access materials the DPA 1998 did not oblige to publish and which he could not require access to since he was not a Royal Free's patient. In other words, control was taken by citizens rather than data subjects whose health data is being processed. Furthermore, the fragmentation of the Trusts' assessments is invisible for their data subjects because a patient is only the data subject of one Trust at a given time. Even if the Trusts, such as Yeovil and Taunton, share their patients, the assumption for a patient is likely to be that the two controllers have the same assessment. A patient may not even imagine that there could be inconsistencies in the Trusts' approach to the same clinical use of the same app built by the same data processor, DeepMind. Also, patients, as most data subjects, are unlikely to have the technical expertise and the time to 'digest […] complex information about computational systems'"[154] In that sense, collective action could prove more effective than individual actions stemming from just data subjects.

The *Digital Rights Ireland* and *Schrems* cases are a vivid example of 'the success of grassroots civil liberties organisations and citizen movements' under the Directive and now the GDPR.[155] The new Article 80(1) GDPR now expressly allows data subjects to mandate a 'not-for-profit organisation active in the field of the protection of data subjects' rights and freedoms'. Article 80(2) GDPR goes even further: NGOs can launch legal action before the supervisory authority without a mandate from a data subject. Data subjects can thus be supported without getting involved and potentially without their prior knowledge.

This evolution in the law could be lamented as an admission of defeat by the GDPR and an example of internal contradiction, where data subjects cannot be expected to control their data and challenge controllers' processing decisions. Alternatively, it could be viewed as taking a pro-active step into building what is not an architecture of control but an architecture of custody: others are made custodians to protect data subjects. Yet, these organisations may prove as limited as data subjects in their oversight since Articles 13 and 14 GDPR, and their former equivalent, do not require the publication of risks assessments and contracts.[156] Viewed through the lens of the GDPR developing architecture of custody, more transparency as to risks and contracts could however be argued as an essential element to ensure that data subjects and citizens are able to contest controllers' decisions on the processing. How these NGOs could be in practice empowered is nevertheless beyond the scope of this paper.

4.2.2 *The fundamental role of auxiliary custodians under the GDPR*

Under the DPA 1998, and the Directive, processors, had no obligation other than securing a contract for security purposes and complying with the Trusts' instructions. So for Streams, DeepMind had no legal obligation to pinpoint to each of the Trusts

[154] Veale, Binns, and Ausloos. (n 26) 121, 105; L Edwards and M Veale, 'Slave to the Algorithm? Why a "Right to an Explanation" is Probably Not the Remedy You Are Looking For' (2017) 16 Duke L & Tech Rev 18
[155] Lynskey (n 23) 261. Schrems II is both under the Directive and the GDPR.
[156] Article 29 WP (n 90)

that their assessment on proportionality and necessity contradicted each other and may create a number of risks: risks for the data subjects, and risks for DeepMind itself as it needed to keep track of how it implemented four different sets of instructions stemming from four different assessments.

With the GPDR, processors are now under an obligation 'to assist the controller in ensuring compliance' with notably the DPIA process and the controllers' duty to facilitate data subjects' rights.[157] In addition, under Article 28(3)(h) GDPR, they must point out to controllers that 'an instruction infringes th[e] Regulation'. Processors should actively support controllers, not just passively implement their instructions. The GDPR brings a dynamic between processors and controllers, that is best viewed as facilitating effective custody among the different actors involved in the decision-making process on the processing.

For DeepMind, now Google Health, we argue that the transformation of processors into auxiliary custodians brings significant changes. Not only DeepMind should be pointing out the lack of compliance to each of the Trusts, but it could also be argued that it has a responsibility to bring awareness to all the Trusts currently using Streams of the fragmented assessments as this fragmentation undermines the legitimacy of the Trusts' decisions on processing. It could even be argued that Google's decision to stop publishing the contracts and to refer data subjects to Google's standard privacy policies related to the use of a Google account, but not to Streams,[158] violates its duty, as processor, to assist controllers in demonstrating compliance and facilitating data subjects' right to information.

For the Trusts, the change brings a new perspective on how to choose their processor and view their relationship over time. Article 28(1) GDPR requires them to choose processors with 'sufficient guarantees' that the 'processing will meet the requirements of the Regulation'.[159] The Trusts could examine the absorption of DeepMind by Google in November 2018 not only in light of the technical capabilities of Google to implement their instructions but also in light of its capacity to signal to the Trusts GDPR's violations. Such questions would oblige Google to formulate how it approaches compliance for Streams, in light of: first, the total absence of specific information about Streams across its three websites (DeepMind, Google Health which refers to Google pages); and second, the 50 millions euros fine imposed in January 2019 by the French data protection regulator (CNIL) for structural lack of data protection information to Google users.[160] As primary custodians choosing auxiliary custodians, controllers such as the Trusts should be empowered to ask awkward questions.

4.2.3 The supervisory authority's role in supporting primary custodians

The role of national supervisory authorities has always been seen as important to the data protection framework under the Directive, and the GDPR, by strengthening their

[157] Article 28(3)(f) and (e) GDPR.
[158] Supra section 3.3
[159] Article 17 Directive focussed solely on data security; Schedule 1 (Part II) DPA 1998.
[160] In 2018, the CNIL fined Google 50 million euros, for lack of transparency, inadequate information and lack of valid consent regarding ads personalisation at https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc . The Irish Data Protection Commission has opened an investigation on 22 May 2019, Simon Carswell, 'Data Protection Commission opens first investigation into Google', *The Irish Times* 22 May 2019 at https://www.irishtimes.com/business/technology/data-protection-commission-opens-first-investigation-into-google-1.3900961 Google was investigated by the CNIL, upon request by Article 29 WP, Letter of 16 October 2012 on Article 29 WP website (now archived) and was found non-compliant.

powers, has intended to promote monitoring and 'strong enforcement'[161] as 'an essential component of the protection of natural persons'.[162] Monetary penalties of up to 4% of the word-wide turnover leave no doubt that GDPR violations should bring serious fines rather than the meagre penalties that were previously applicable (for example, £500,000 under the amended DPA 1998 in the UK). Strong enforcement is not seen as an obstacle to innovation but as an integral element to push controllers to build innovations centred on data protection by default. Article 57 GDPR also widens the supervisory authorities' duties to include non-enforcement tasks, for example: to raise awareness of the GDPR requirements among the public and controllers and processors; to advise controllers during the DPIAs process as per Article 36 GDPR, or to adopt standard contractual clauses for controllers and processors to use as per Article 28 GDPR. Regulators have therefore a supporting role: towards data subjects who complain; and towards controllers and processors in order for these actors to protect data subjects. As importantly, regulators should view their role as an active one at the centre of the GDPR's architecture of custody: they are not limited to the tasks listed in Article 57 GDPR since the last task is to 'fulfil any other tasks related to the protection of personal data'.

In the UK, under the DPA 1998, the ICO has been pro-active in some areas, having been notably one of the first national supervisory authorities to promote privacy by design and privacy impact assessments as good practice with associated guidance. In terms of enforcement, however, questions have been raised as to the ability of the ICO to impose the DPA 1998 requirements or to actively support good PIAs for example.[163] More recently, in October 2019, criticisms before the Joint Committee on Human Rights investigating the 'Right to Privacy and the Digital Revolution' centred on the enforcement gap, several witnesses calling for a 'proactive implementation and enforcement where there is blatant noncompliance' and for the ICO to be more imaginative in its processes and structure 'if abuses are to be identified and effectively prosecuted'.[164] The Committee thus recommended a review of the measures in place to enforce the GDPR and DPA 2018, including whether the ICO has enough resources.[165]

Our analysis in section 3 on the shortcomings of the Trusts has revealed some puzzling choices the ICO made and which seem to echo the criticisms expressed before the Joint Committee. Regarding the monitoring process of Royal Free, we have demonstrated that the Linklaters report, published in June 2018, after the GDPR came into force on 25 May 2018, presented some serious misinterpretations of the DPA 1998, GDPR and ICO's guidance. The ICO carefully stated that it did not endorse the conclusions of the report, but it has never mentioned that some of the interpretations on the processing's necessity and proportionality -at the heart of controllers' obligations- were unsustainable. However, it sought legal advice on another legal matter and concluded that the report was mistaken in its interpretation of the duty of confidence.[166] The contrast with ICO's silence on data protection,

[161] Recital 7 GDPR: EU Commission (n 30)
[162] Recitals 117, 123, 129 GDPR.
[163] For PIAs, citing Warren & Charlesworth, Wright, D., Finn, R. and Rodrigues, R., 'A comparative analysis of privacy impact assessment in six countries' (2013) 9(1) Journal of Contemporary European Research 161 at http://www.jcer.net/index.php/jcer/article/view/513
[164] Report (n 101) 31 para 101, 103.
[165] Report (n 101) para 105, p31
[166] ICO, 'Royal Free NHS Foundation Trust update, July 2019,' 31 July 2019 at https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/royal-free-nhs-foundation-trust-update-july-2019/

combined with the ICO's declaration that Royal Free is now compliant including for the clinical use of Streams, is likely to be interpreted as a sign of the quality of the report when it partially failed. Given the media attention the Streams project attracted, and the use of the report on Royal Free's website to reinforce the Trust's message of compliance, the ICO's choice to stay silent is arguably dangerous, unwittingly misleading Royal Free and other Trusts which wish to use Streams as to what the GDPR requires.

We argue that silence here was not an option; whichever legislation is considered. Under s51 DPA 1998, the ICO was required 'to promote the observance of the requirements of this Act by data controllers. Under Article 57 GDPR, regulators ought to promote controllers' and processors' awareness of their obligations and ensure compliance. The auditing report may have no binding authority or persuasive authority in the eye of the law, but its publication as part of a compliance process which the ICO initiated and structured carries for the regulator a responsibility to indicate whether or not the report contained some glaring misinterpretations. As importantly, one of the mistakes made in the report – that Article 9(2)(h) GDPR can justify the testing of the app, where it can only justify the clinical use of the app- is so fundamental that it begs the question as to whether the ICO has read the report and/or whether it has relinquished its enforcement and advisory duties to a private law firm which in this instance is unfit for purpose. The silence here failed the controllers: not just Royal Free, but also the other Trusts who may rely on the report. The ICO has not supported them. Nothing in the GDPR, DPA 2018, and in the former DPA 1998, prevented the regulator from publishing its own report and indicating which legal grounds Royal Free could use and recap on the other aspects of the assessment. More importantly, if we see the GDPR as strengthening the architecture of custody that the Directive, transposed in the DPA 1998, had started to create, then the ICO ought to have acted differently so that its silence could not be interpreted as implicitly (albeit unwittingly) condoning the report. Furthermore, if the ICO's silence stems from a lack of resources – in that it did not have the money and/or the staff to analyse in details the Linklater's report-, then it should consider speaking up and report to the Government and the Parliament.

Another aspect of the ICO's actions in the Streams project raises some questions as to what should or could be expected of the ICO and how it is in a position to support controllers effectively and thus data subjects. All Trusts indicated that they consulted the regulator in the course of conducting their DPIA; however, none have the same assessment. This begs the question as to how the hospitals have communicated with the ICO and to which extent the regulator was in any position to seriously consider the DPIAs, whether under Article 21 Directive or under Articles 35 and 36 GDPR. A related question is whether the regulator has the structures and processes in place to conduct its consulting role freely when the same regulator may receive a few months later a legal complaint about the processing it had been consulted. Indeed, the ICO does not strictly differentiate between its ex-ante role at the DPIA stage, and its post-facto monitoring and enforcing functions. Neither the Directive nor the GDPR envisages this potential conflict of objectives within the supervisory authority. It will thus fall on supervisory authorities like the ICO to build mechanisms to avoid such conflicts. The ICO would not be the first regulatory authority in that position, and it should not come as a surprise: it is a sign of the regulatory framework maturing. The former Financial Services Authority, now the Financial Conduct Authority, has established a Regulatory Decisions Committee (RDC) to separate its

decisions on investigation and compliance, from those on authorisation and certification.[167] Given the level of monetary penalties the GDPR allows the ICO to impose and which is not unrelated to that of penalties imposed by the FCA,[168] the ICO may want to take a more active role in preventing potential conflicts of interests.

5. Findings and conclusion

This detailed analysis of the data protection framework surrounding the Streams app highlights the inherent difficulties for the NHS to balance what are effectively conflicting duties of, on the one hand, protecting their patients' data and, on the other hand, the push for innovation to provide care. This article has focused on an unexplored aspect of the debate: the protection of patients' data in direct care under the former Directive, the GDPR and the UK DPA 2018. As the former Directive, the GDPR prohibits the processing of health data, including the collection of the data, and imposes stringent requirements should the processing be justifiable. We have demonstrated that these requirements are not so much representative of an architecture of control than part of an architecture of custody. We argued that the vocabulary of control does not do justice to the letter and spirit of the law because it fails to reflect the articulation of the duties allocated to all participants.

Firstly, the law recognises the reality that the data controllers, not the data subjects, are the initial decision-makers. Hence, it assigns the primary responsibility of compliance on the data controllers. The word 'controller' itself may unwittingly mislead on how to interpret this responsibility. When exerting control over processing, controllers may focus too much on the interests of their organisation, thus losing sight of their duty to protect data subjects, especially when the latter is in an unfavourable asymmetric relationship of power. To ensure this delicate balance is maintained, we propose to view controllers as primary custodians. The Streams example highlights patches of compliance, depending on the requirements and on the Trust considered. The result is the fragmentation of the Trusts' individual assessment, which undermines the legitimacy of their approach to necessity and proportionality. In this context, we argue that architecture of custody provides the means for interpreting the legal requirements as well as a direction as to what controllers should do when the law itself provides 'get-out clauses' or recommends a course of action without creating corresponding legal duties. In Streams, for the Trusts to consider themselves as primary custodians would push them to adopt a holistic approach and develop ways to implement the spirit of the law as much as the letter.

Secondly, controllers are not isolated. Processors are now, under Article 28(3) GDPR, auxiliary custodians, with a duty to ensure compliance for themselves and the controllers. This shift implemented by the GDPR transforms the relationship between controllers and processors. Processors are no longer passive recipients of instructions but are an essential component in the dynamics of compliance. We argue that controllers, such as the Trusts, should require processors like DeepMind or Google Health UK, to be pro-active in ensuring that the processing represents a

[167] See https://www.fca.org.uk/about/committees/regulatory-decisions-committee-rdc. In 2018 and 2019, the FCA also published two documents, one for its approach to Enforcement and one for its approach to Authorisation, at https://www.fca.org.uk/publications/corporate-documents/our-approach. See G Treverton-Jones, A Foster and S Hanif, *Disciplinary and Regulatory Proceedings* (9 edn, Jordan Publishing, 2017), part 1

[168] See for 2019 https://www.fca.org.uk/news/news-stories/2019-fines

balanced approach between the needs of the organisations and the protection of the rights and interests of the data subjects.

Thirdly, the law's emphasis on data subjects' control unwittingly masks the features empowering others than the data subjects in ensuring compliance. It distracts from the recognition, in the GDPR, of what was initially developed as an informal practice under the Directive: the legal actions brought in by NGOs. The Streams project illustrates how these actors play a fundamental role in supporting data subjects. The shortcomings of the project only came into light because of the intervention of journalists and other third-parties challenging the Trusts' decisions. In other words, the law empowers citizens as part of the architecture of custody.

The final element of our proposal for interpreting the data protection framework is to view the regulator as a fundamental component of this architecture. The Streams project highlights how the puzzling choices the ICO made can lead to questioning its capacity not just to protect data subjects but also to support controllers and processors in making the best decisions as custodians. We argue that the ICO's silence on some questionable interpretations of the law and its guidance by the auditing firm failed to provide adequate support to controllers as well as the data subjects. Moreover, Streams illustrates the current limits of the law where the GDPR, no more than the Directive, acknowledges the conflict of interests arising from the cumulative roles of adviser and enforcer for the regulator.

While public health authorities need to be able to use technology efficiently for the public good, it has to be in a way that preserves patients' rights. Viewing the law as an architecture of custody transcends the limits of a discourse which emphasises the data subjects' control. It reveals how all participants of the framework have a custodial role to play and should collaborate in ensuring the balance between the free flow of data and the data subjects' rights and interests as per Article 1 GDPR and former Directive.