

Central Lancashire Online Knowledge (CLoK)

Title	GPs, Patients and Health Data Commercialisation in England
Type	Article
URL	https://clock.uclan.ac.uk/31386/
DOI	10.31031/TTEH.2022.03.000568
Date	2022
Citation	Fisk, Malcolm (2022) GPs, Patients and Health Data Commercialisation in England. Trends in Telemedicine & E-health, 3 (4). ISSN 2689-2707
Creators	Fisk, Malcolm

It is advisable to refer to the publisher's version if you intend to cite from the work.
10.31031/TTEH.2022.03.000568

For information about Research at UCLan please go to <http://www.uclan.ac.uk/research/>

All outputs in CLoK are protected by Intellectual Property Rights law, including Copyright law. Copyright, IPR and Moral Rights for the works on this site are retained by the individual authors and/or other copyright owners. Terms and conditions for use of this material are defined in the <http://clock.uclan.ac.uk/policies/>

GPs, Patients and Health Data Commercialisation in England

ISSN: 2689-2707



***Corresponding author:** Malcolm Fisk, Centre for Computing and Social Responsibility, De Montfort University, England

Submission:  August 30, 2022

Published:  September 12, 2022

Volume 3 - Issue 4

How to cite this article: Malcolm Fisk. GPs, Patients and Health Data Commercialisation in England. Trends Telemed E-Health. 3(4). TTEH. 000568. 2022.
DOI: [10.31031/TTEH.2022.03.000568](https://doi.org/10.31031/TTEH.2022.03.000568)

Copyright@ Malcolm Fisk, This article is distributed under the terms of the Creative Commons Attribution 4.0 International License, which permits unrestricted use and redistribution provided that the original author and source are credited.

Malcolm Fisk*

Centre for Computing and Social Responsibility, De Montfort University, England

Abstract

The advent of Artificial Intelligence (AI) and, more specifically machine learning, brings great opportunities for healthcare. But linked with this there are unresolved issues about the safeguarding of patients' personal (including health) data as the frameworks for their use appear to allow for their sale by or transfer from the National Health Service (NHS) to commercial organizations. The trust that most patients hold in the NHS may, as a consequence, be undermined and lead many of them to 'opt out' of (or choose not to 'opt in' to) the systems for data collection and sharing that are being configured in England by the UK government. For those AI suppliers and service providers that are seeking patients' health data, challenges may as a consequence of 'opt outs' arise because of the potential inadequacy (limited size or representativeness) of the datasets that would otherwise be available. For the patients in question, there are concerns that include the ownership, privacy and confidentiality of their data, together with the seeming shortcomings of NHS and government plans for a framework that would facilitate data sharing in ways that recognize their particular circumstances and the different levels of confidentiality that might apply. There is, at the same time, some evidence of patient trust in public health services being conditional on their data being in the firm control of the NHS-with strong resistance to data being used for financial gain by commercial organizations. This brief communication offers a preliminary examination of the issues from the point of view of patients and their General Practitioners (GPs) in England. And in light of limitations of the UK Government's June 2022 Policy Paper 'Data Saves Lives: Reshaping Health and Social Care with Data', it calls for the urgent development and adoption of mandatory regulatory frameworks that will (a) cement the role of GPs' as guardians of patient data; and (b) provide appropriate safeguards for patients.

Keywords: General practitioners; Patients; Data; Artificial intelligence; Machine learning; Privacy

Abbreviations: AI: Artificial Intelligence; NHS: National Health Service; GP: General Practitioners

Introduction

Concerns about the commercialisation of patient data in the UK date to the early period of computerisation in hospitals and general practices. At this time, initial experiments in Devon (southwest England) were followed by the government's 'Micros for GPs' scheme launched in 1982. As a result of this scheme, two commercial companies, VAMP and AAH Meditel, selected 'on the basis that their hardware and software were British' [1], offered 'multiuser' computer systems to GPs at no cost subject to their agreement to 'collect and provide comprehensive data about morbidity, drug prescribing, and side effects' [2]. Many GP practices were eager to take up the offer-the proportion of them with computers rising, as a consequence, to 96% by 1996 [3]. Early barriers to the adoption and usage of computers and, ipso facto the need to move to digitized patient data records included a reluctance of GPs to be pushed into arrangements whereby they were obliged to collect data that could then be sold to pharmaceutical companies [4].

Methods

The focus of this communication is concerned with the value that is being attributed to patient data (whether sourced from paper, images or digital records) in the context of rapid

increase in use of AI (more specifically machine learning). The communication does not follow any specific scientific process except for drawing on the outcome of systematic searches undertaken online by the author; and his consultations with a small number of GPs. The selection of the topic of commercialisation of patient data reflected both its importance and the attention given to it in the UK government's 2022 policy paper 'Data saves lives: Reshaping Health and social care with data' [5]. Touched on are therefore

- a) The extent to which commercial organisations are envisaged as partners in, with or contracted to NHS services and potentially able to 'benefit' from patient data.
- b) The appropriateness of the NHS operating an opt-out system whereby patient agreement for the use of their data is assumed to be given unless it is notified to the contrary.
- c) The extent of patient trust in the NHS (and, more specifically, their GPs) in a context where commercial organisations may be in receipt of their data.
- d) The position and moral responsibilities of GPs as guardians of patient data.

Results

This communication does not challenge what is a range of undoubted benefits that will arise from AI in healthcare. Some such benefits have been highlighted by Topol in the identification, for instance, of skin cancers based on image analyses [6]. Such analytical techniques, he stated, were 'empowering the family physician and general practitioners'. What is clear in the broader context is that many claims that are made for AI relate to analyses of large sets of data. The use of historic patient records has sometimes been helpful to underpin such analyses and for which issues of privacy, though important, can be more easily overcome. But there remain questions about the robustness and representativeness of the data that are utilised for the patient populations or groups for whom better treatment outcomes are sought [7]. A broader debate about this robustness and related matters of bias is now taking place. What is in focus in this communication is the matter of data sharing and the commercial 'market' for those data. This is a matter of concern to GPs-not simply because of the data that they hold, but because of their moral responsibility for its safeguarding [8]. General practices, per the policy paper, will be obliged to share patient data. But in a context of often opaque techniques for its analysis (through machine learning), GPs are unlikely to be able to give reassurances to patients about the way their data are being used or the way in which treatments offered by them are informed by the outcomes of analyses of those data. The context is one where the lack of explicability of machine learning has been emphatically pointed to [7], with Verdiccio [9] affirming that 'if doctors do not understand why the algorithm made a diagnosis, why should patients trust the recommended course of treatment?'

If GPs accede to sharing patient data in the manner intended by the UK government, the question arises as to whether patient trust in the NHS will be undermined? Research undertaken in 2016

found [10], albeit from just three workshops, that people felt it 'particularly difficult to accept commercial organisations having access to' even anonymous patient-level data. People's desire was for greater regulation, essentially because of the worry that 'unscrupulous commercial organisations... might not adhere to the regulations that are in place'. More recent work with patients in two workshops and a patient questionnaire (with over 300 responses) [11], found people had 'greater reservations about [sharing health data with] industry' than other types of organisation; and a 'central concern' regarding 'unauthorized data use'. It is clear and obvious that patients are sensitive about their personal (including health) data and, therefore, are legitimately concerned about the manner in which data sharing, usage and analysis takes place. With regard to any loss of trust in the NHS, some of this may have already taken place-with a dramatic fall in people's satisfaction with GP services from 68% in 2019 to 38% in 2021 (per a major national survey) albeit that this, in part, resulted from the restrictions on face-to-face consultations during the COVID pandemic [12]. But the importance of any diminution in trust in the context of data-sharing cannot be readily overstated. It was a lack of adequate attention to this matter that led to the collapse of the UK government's 2013 care.data project (that aimed 'to aggregate or share all general practice patient records to create a data set capable of supporting data-intensive biomedical research'). Many GPs therefore 'opted out alongside patients' [13]. Now, nearly a decade later, the amount of health data available to GPs and other clinicians is much greater. But so are the potential consequences if those data are not effectively safeguarded.

It is conceivable that with the right kind of regulatory frameworks in place (and their enforcement) that patient trust in the NHS (and GPs) might be retained or reinforced. But, for England, much work needs to be undertaken (with urgency) in the face of rapid developments around AI and the increasing pressures for data sharing to facilitate their analysis. The fact of the matter is that if trust is lost because the frameworks for the safeguarding of data are not robust, GPs are likely to support patients in opting-out of data sharing (as they did for care.data). One potential consequence is that the size of anticipated datasets (potentially impacting the robustness of AI analyses) will be reduced. Of some assurance is the UK government's Policy Paper [5] promise (following 'work with the public') of a 'data pact' to 'explain more clearly how data (are) being used across the health and care system' and a commitment (though not until December 2023) to 'commercial principles to ensure that partnerships for access to data for research and development have appropriate safeguards and benefit the public and the NHS'. Little is said, however, of the risks of AI (though more is promised in a White Paper for 'later' in 2022). A question remains, furthermore, as to what form any 'partnerships' with commercial organizations might take. What the 'terms' are in place, at least for contracts with data processing companies, can in any case be difficult to discover. These have been pointed to as 'networks of secret agreements' [14].

The range of commercial bodies, with AI expertise, that are in the hunt for patient datasets is, meanwhile, extensive and

includes some commercial giants. Google's 2015 deal (through their company Deep Mind) to obtain 1.6 million patient records (of acute kidney injury) from the Royal Free London NHS Foundation Trust was an alert for clinicians and health professionals of all kinds to consider (a) the value of the data they hold; and (b) the vulnerability of their patients to the loss of those data. This deal was investigated by the Information Commissioner's Office (the UK's watchdog) - with lessons learnt and practices changed. The broader context must not be overlooked. More and more patients are integrated into our increasingly digital world. Many are users of smart phones, wearables, voice assistants and varied devices in the home. They have ready access to health information and are increasingly equipped to make choices regarding their care and about their personal (including health) data. GPs, meanwhile, have a special responsibility for the personal data (whatever their origin) of patients. The question now arises, therefore (and with the threat of commercialisation in mind) as to when, how and in what circumstances is 'ownership' of patient data transferable to other parties? This communication holds, in the first instance, that the data are owned by the patient and, for the purpose of health care, are (normally in the first instance) entrusted to GPs. To think otherwise leaves the door wide open to what Cohen [14] referred as 'bioprospecting' by bodies with narrow commercial interests for data and who 'express unquestioned assumptions about their rights to appropriate and exploit that which is freely available'.

Discussion and Conclusion

The point regarding the undoubted benefits of AI in healthcare has been made. It follows that there can be benefits from the sharing of accurate, robust and representative data in a way that supports AI (and machine learning) outputs. At the same time, people's sense of privacy combined with their trust in the NHS, require appropriate protections for their personal (including health) data. It is argued that, ideally, such protections would be sensitised to each person's different and changing circumstances and needs. The required open discussion about this has yet properly to take place. But, at the least, it should take us away from any narrow pursuit of 'data-led' health services and from the blunt application of an opt-out framework that might expose patients to the exploitation for profit of their health data. Arguably, an opt-in (rather than opt-out) framework, responsive to the different circumstances and wishes of patients, is required. This could, with the appropriate consents, explore the when, how, with whom and in what circumstances patient data could be shared - and by which the care and support they receive (whether or not informed by AI) would be facilitated. The parameters to underpin such an opt-in system would help to (re)build patient trust. A fundamental requirement would be alignment with the current practice of GPs but informed by patient choices about the level of confidentiality they wish for their data regarding

- a) Matters that may carry a stigma or offer the potential for discrimination

- b) Different circumstances (of e.g., acute need) that could arise
- c) Considerations of especial risk or vulnerability (e.g., due to frailty, mobility, cognitive or sensory impairment)
- d) Family and household relationships

This communication, in signaling the importance of the agenda of commercialisation of patient data, has highlighted issues of privacy, data ownership and the responsibilities of GPs in England. Consideration of the matter in relation to GPs has been apposite in view of their being, for most patients, the trusted 'face' of the NHS. However, the direction being signaled for the NHS (in the policy paper) carries the potential to put patients' (already eroded) trust in jeopardy. The further consultations pointed to in the Policy Paper must, therefore, take place with some urgency with a view to establishing if there is clear evidence for a stepping back from a narrow commercial ('data-driven') approach for the NHS to one that embraces a more nuanced perspective - both retaining safeguards around patient data and harnessing the benefits of AI.

References

1. Curtis P (1984) Computers in British general practice. *Journal of Family Practice* 19(1): 98-103.
2. Benson T (2002) Why general practitioners use computers and hospital doctors do not-part 1: Incentives. *BMJ* 325(7372): 1086-1089.
3. Preece J (2000) The Use of Computers in General Practice. In: (4th edn), Churchill Livingstone Publishers, UK, pp. 1-356.
4. Tudor-Hart J (1988) A new kind of doctor. Merlin Press, Georgia, pp. 1-308.
5. (2022) Department of Health and Social Care. Data Saves Lives: Reshaping Health and Social Care with Data, UK.
6. Topol E (2019) Deep medicine: How artificial intelligence can make healthcare human again. Hatchett Book Group, USA, pp. 1-314.
7. Rosemann A, Zhang X (2022) Exploring the social, ethical and legal responsibility dimensions of artificial intelligence for health-A new column in intelligent medicine. *Intelligent Medicine* 2(2): 103-109.
8. Salisbury H (2021) Should GPs break the law on data privacy? *BMJ* 373:1451.
9. Verdicchio M, Perin A (2022) When doctors and ai interact: On human responsibility for artificial risks. *Philosophy and Technology* 35: 11.
10. Chico V, Hunn A, Taylor M (2019) Public views on sharing anonymised patient-level data where there is a mixed public and private benefit. *NHS Health Research Authority*, pp. 1-43.
11. Atkin C, Crosby B, Dunn K, Price G, Marston E, et al. (2021) Perceptions of anonymised data use and awareness of the NHS data opt-out amongst patients, carers and healthcare staff. *Research Involvement and Engagement* 7(1): 40.
12. Rachel W (2021) 2021 GP Patient Survey Results Released. Ipsos Mori, p. 1.
13. Roberts C, Mackenzie A, Mort M, Theresa A (2019) Living data: Making sense of health biosensing. Bristol University Press, UK, pp. 1-208.
14. Cohen JE (2018) The biopolitical public domain: The legal construction of the surveillance economy. *Philosophy and Technology* 31: 213-233.

For possible submissions Click below:

[Submit Article](#)