Original Research Article

BIG DATA & SOCIETY

Big Data & Society
January–June 2017: 1–12

DOI: 10.1177/2053951716688490
journals.sagepub.com/home/bds
SAGE

Understanding the care.data conundrum: New information flows for economic growth

Paraskevas Vezyridis and Stephen Timmons

Abstract

The analysis of data from electronic health records aspires to facilitate healthcare efficiencies and biomedical innovation. There are also ethical, legal and social implications from the handling of sensitive patient information. The paper explores the concerns, expectations and implications of the National Health Service (NHS) England care.data programme: a national data sharing initiative of linked electronic health records for healthcare and other research purposes. Using Nissenbaum's contextual integrity of privacy framework through a critical Science and Technology Studies (STS) lens, it examines the way technologies and policies are developed to promote sustainability, governance and economic growth as the de facto social values, while reducing privacy to an individualistic preference. The state, acting as a new, central data broker reappropriates public ownership rights and establishes those information flows and transmission principles that facilitate the assetisation of NHS datasets for the knowledge economy. Various actors and processes from other contexts attempt to erode the public healthcare sector and privilege new information recipients. However, such data sharing initiatives in healthcare will be resisted if we continue to focus only on the monetary and scientific values of these datasets and keep ignoring their equally important social and ethical values.

Keywords

National Health Service (NHS), consent, care.data, ethics, contextual integrity, assetisation

Introduction

In every part of the world, states work to find ways to open up and analyse the data they have been gathering about their citizens and services, because they believe it will have a transformative effect on knowledge and services (Verhulst et al., 2014). For example, in healthcare such data initiatives tend to focus on creating value through service efficiencies by sophisticated business intelligence, improved healthcare practices and biomedical innovation (DH, 2011). In the UK, it is estimated that analysing data from NHS electronic health records (EHRs) could result in efficiency gains of between £16.5 and £66 billion per year, while transforming the service to a more proactive and personalised one (Bosanquet and Evans, 2014). This commitment to generate wealth out of NHS health data (DH, 2012b; HM Government, 2012) is also evident in calls to develop policy frameworks and information technology (IT) infrastructures that facilitate closer collaboration between the NHS and commercial bioscience firms (BIGT, 2003; HITF, 2004) in order to accelerate biomedical research and reduce costs (Pathak et al., 2013).

One such health data sharing initiative in the UK was care.data,[1] a programme of work for the development of a central database with linked NHS hospital and general practice (GP) records. Led by NHS England and implemented by the Health and Social Care Information Centre (HSCIC) it has the purpose of collecting, de-identifying and linking datasets across the NHS (Grace and Taylor, 2013). HSCIC, now called NHS Digital, is an executive non-departmental public body established by the Health and Social Care Act (HSCA) (DH, 2012a) to replace NHS Connecting for

Nottingham University Business School, UK

Corresponding author:
Paraskevas Vezyridis, Nottingham University Business School, Jubilee Campus, Wollaton Road, Nottingham NG8 1BB, UK.
Email paraskevas.vezyridis@hotmail.co.uk

Health and the NHS Information Centre. Sponsored by the Department of Health, it provides informational infrastructure to the NHS so as to collect centrally its electronic health and social data for various analyses and national statistics about population health and service operation (Health Information and Quality Authority, 2014). For care.data, it will collect identifiable information, such as the NHS number, date of birth, postcode and gender, as well as healthcare information, such as family history, vaccinations, biological values, diagnoses, referrals and NHS prescriptions. In the future, it aims to offer the service of linking the pseudonymous datasets it holds to datasets supplied by customers (Nuffield Council on Bioethics, 2015).

Since 90% of patient care is non-hospital, care.data will collect a wealth of sensitive personal health and administrative data (Hoeksma, 2014) so as to support whole population research for developing effective care pathways and service models.[2] The programme, however, was stalled in February 2014 due to ethical concerns, particularly in relation to its information governance framework and data sharing arrangements. It was eventually abandoned in July 2016 (Freeman, 2016). At first, it appears that HSCIC was forced to postpone its plans for extracting and linking primary and secondary care data because of certain privacy, and (we argue) commercial, concerns.[3] This became more evident after a public outcry due to a notable data sharing fiasco from its predecessor where hospital data was sold to actuaries (Donnelly, 2014).

To study the controversies and the resistance to this programme by the public and (some) healthcare professional bodies alike, we first apply Nissenbaum's (2010) conceptual framework of contextual integrity (CI) to privacy by paying particular attention to the technology and policy-making that has placed HSCIC in the centre of NHS information exchanges. We use this framework to describe what new information flows care.data aspired to introduce between data subjects, senders and recipients of information as well as new principles and norms for the public healthcare context. We also attempt to show how certain actors in the wider political-economic context value this data and attempt to erode the public healthcare context so as to privilege other goals and ends. We do this by examining how certain actors and their interests shaped the direction of the programme for the transferring of data to the private (healthcare) sector from the public healthcare sector.

Therefore, we also treat care.data as a political-economic as much as a technical or ethical phenomenon (Davies et al., 2013). As critical STS scholars have demonstrated with biomedicine and, generally, with life sciences (Cooper, 2008), EHRs under care.data appeared to follow a similar path of capitalisation. They depict the same threefold relation between knowledge and value: the ethical value of improving health, accountability audits for better services and the monetary transactional value of innovation (Rajan and Leonelli, 2013). For the private sector, such scientific and economic endeavours are always risky and politically sensitive which means that the private sector will not fully engage with them from the outset. Therefore, this new state-driven data sharing initiative carried its own normative assumptions of size and speed (Davies et al., 2013) to justify its necessity (Lezaun and Montgomery, 2015). It also attempted to instil what we consider (and present below) a new set of *duties* for patients–citizens and the public healthcare sector.

Such big personal health data sharing programmes, we argue, expect patients and professionals to share as much personal healthcare information as possible within the circle of care. The NHS is increasingly obliged to collect and disseminate datasets for administrative and research purposes that may go beyond the context and operation of the public healthcare sector. Preferred economies of scale, available infrastructures, organisational capabilities, public engagement strategies and business modelling envelope this context and *transactionalise* its principles for new, de-contextualised information flows. In a political-economic context of increased public services privatisation and austerity, the above duties are gradually shifting the obligations of citizens, healthcare professionals and the NHS (with regards to the collection and analysis of personal health information) from the requirements and needs of the individual as a member of the society, to those of bigger actors (i.e. the state, market, science) for the assetisation of NHS primary care datasets and their introduction into the knowledge and commercial economies. In this way, we believe we provide a new and useful approach in overcoming the NHS data sharing conundrum, which is located in a *divisive* rhetoric of privacy *against* healthcare improvement and economic prosperity, and show why such initiatives are resisted and will continue to do so in the near future.

Contextual approach to privacy

Nissenbaum (2010) developed the framework of CI to study, from a moral and political point of view, privacy concerns around new social–technical ITs and provide policy solutions to actual problems of information collection, analysis and dissemination. For her, a privacy conundrum should not be about sharing information or not. Such views tend to narrow the discussion down to their differences while we seek ways to sacrifice one over the other (Taylor, 2014). Privacy is about appropriate sharing of information within a given *context* (Nissenbaum, 2010). For example, the type and

amount of information I share with my healthcare professional, and the privacy expectations we both hold around this exchange of information, are different when I move to the context of family or employment. Instead, CI helps us to examine new '*information flows*' and '*principles of transmission*' between '*subjects*', '*providers*' and '*recipients*' that respect the norms and ends of a particular context (Nissenbaum, 2010). Nissenbaum (2010) also acknowledges the fact that people may accept novel information flows, and, as a result, less privacy, if these flows can demonstrate their moral superiority and effectiveness over established ones, without disturbing contextual values. If not, then the integrity of the context is violated.

A final moral and political question that Nissenbaum (2010) calls us to answer when we examine new information flows is who, in the end, are the new recipients of information. This means that the public's resistance to data initiatives may not always be fuelled by the level of information aggregation which an omnibus provider may support, but that this is being achieved in a way that favours stronger actors, who become the new information recipients and can use this information for their own benefit (Nissenbaum, 2010). Consequently, for every system that introduces novel information flows, we need to assess the moral claims and interests of the various actors involved. We need to examine whether, how and to what outcome '*principles attaching to social goods in one sphere intrude into the distribution of goods in another*' (Nissenbaum, 2010: 168). In the case of care.data, we can say that this dispute between the two contexts was highlighted in a recent Health Committee about the handling of NHS data where the Chair of HSCIC explained the perceived conflicting policy framework within which the centre has to operate (House of Commons, 2014):

> *I have two separate drivers, one of which is an open data agenda, which has been pursued by all Governments in the past decade. That agenda is aimed at making as much data available for as many people as possible, in the belief that it will result in significant benefits in terms of improving efficiency within the health care system, and in the wider economy. Against that is a very principled position, and I understand it, of those who say, 'I don't want my data used for that purpose'. That is a totally legitimate discussion that should be undertaken under the new regime.*

The duty to share

In healthcare, one of the most important principles governing transmission of information is confidentiality. This healthcare professional *duty* is based on a mutual agreement that any exchange of information between a patient and a clinician about symptoms and treatments will not be shared with others. There is an expectation, codified in confidentiality agreements, that patients' information does not leave their 'circle of care' (Perera et al., 2011). Although modern healthcare requires increased (electronic) information flows to various professionals and organisations, which might be judged as a prima facie privacy violation, since they permit breaches of previously established informational norms, these are not usually resisted (on the contrary, they are expected) by patients because they are there to support their care. For example, the seventh Caldicott principle makes patient data sharing a responsibility for every healthcare professional in the NHS: '*the duty to share information can be as important as the duty to protect patient confidentiality*' (DH, 2013), while the updated NHS Constitution makes '*every willing patient..a research patient..in the fight against disease at home and around the world*' (HM Government, 2011). Consequently, these new transmission principles that the modern healthcare context supports are considered scientifically and morally superior, in the pursuit of efficient communication, so as to provide patients with the best possible care while running a cost-effective service.

Moreover, clinicians and researchers are expected to practice under professional codes of ethics. As custodians of data they operate under specific rules of confidentiality. They have also developed consent procedures that explain the risks and benefits of treatment or research in order to obtain permission from patients. However, it is not the efficacy of consent itself that has established its virtue in healthcare, but rather the trust patients warrant to these professionals and institutions insofar as they are thought to be doing the best they can to improve their health (Nissenbaum, 2011). They trust the whole system (Dixon-Woods and Tarrant, 2009). Informed consent, then, is a token that does not necessarily symbolise their understanding of research aims (Dixon-Woods et al., 2007) and treatments, but their *commitment* to the practices of those responsible for their well-being, and a token of respect for their autonomy. Therefore, until now, transmission principles in the healthcare context usually involved information shared voluntarily for treatment or research, requiring the knowledge and permission of the patient (Nissenbaum, 2010). Whether proposed uses fell within the scope of the original consent depended on what was '*proposed scientifically, expectations of participants, and social mores at the time of an application*' (Laurie, 2009: 1676).

Driven by the principles of the healthcare context, such as fairness and beneficence (Chan and Harris, 2009), it seems that most patients would probably

participate in healthcare research (even via their health records and without explicit consent) to support those institutions that support their health, and for the public good (Carter et al., 2015). Giving their healthcare data for research purposes (or at least not opting out), especially in the context of a national health system, is understood as an act entailing reciprocity (Busby and Martin, 2006). Despite the fact that in the UK there are other similar (academic and not-for-profit) NHS data sharing initiatives, such as QResearch, ResearchOne and CPRD,[4] that are facilitating public health research from GP records; these have not attracted the public criticism and opposition that the care.data initiative did (Clemence et al., 2013). The public and healthcare professionals are largely supportive of such initiatives for public health research purposes (Torjesen, 2014), although some confusion over issues of confidentiality, data security and legal assurances has been noted (see Brown et al., 2010). In any other case, this *implied* consent would have probably been extended to the care.data initiative but not this time.

The duty to not opt out

An opt-in model is usually considered a more ethical (Willison et al., 2003) approach to active and autonomous decision-making. However, for population-wide studies of low risk or for service planning and auditing, an opt-out model is considered a more scientifically valid and practical alternative (Singleton and Wadsworth, 2006) as it enables bigger and less biased samples (Berry et al., 2012). Healthcare research from EHRs can be greatly enhanced as all data is drawn from the same sample population, thus reducing bias, while revealing inequalities in healthcare (Macleod and Watt, 2008). This is particularly important for difficult to recruit or marginalised study populations (Ridgeway et al., 2013). In any case, when it comes to sharing of NHS data a rigorous opt-out process is expected to serve as the 'ethical minimum' (Sterckx et al., 2015).

In the UK, overriding the common law duty of confidentiality in the NHS is usually possible under Section 251 of the NHS Act 2006. This exemption allows for the disclosure of patient-identifiable data to a third party without patient consent if data will be used for medical purposes, seeking consent is not practical and anonymisation is not possible.[5] The Health Service (Control of Patient Information) Regulations (DH, 2002) specifies that for medical research purposes approvals are granted by the Health Research Authority, while for all other cases responsibility resides with the Secretary of State. However, it was because of the 2012 HSCA and the care.data that data releases to NHS England became *obligatory* for every health and social care provider. Grace and Taylor (2013) note that these mandated data extractions, particularly in relation to the Data Protection Act 1998, the common law duty of confidentiality and the NHS Constitution, may be perceived by patients as an attempt by the government to override, without 'sufficient legal basis', their rights to know how and object to, their confidential data being used for purposes beyond their direct care. In fact, public consultations have pointed to the fact that interested stakeholders would have liked more information: the public about informed choice on participation, GPs about uses for informed education of their patients and researchers about uses for informed applications.[6]

Therefore, this new obligation created pressure on many practices that did not have the resources to fulfil it (Matthews-King, 2014b). Suddenly, the majority of GPs had a responsibility to inform patients about a programme they knew little about (NAO, 2015). As data controllers (and thus legally liable for the patient information they collect[7]) they had an inconsistent statutory obligation both to disclose the data to HSCIC and to process personal data fairly.[8] After increased public pressure, NHS England agreed to do a publicity campaign about care.data to inform the public, but this was restricted mainly to one leaflet per household and some YouTube videos (Triggle, 2014). Moreover, the information provided, which was sent out without proper checks by the programme's Independent Information Governance Oversight Panel (IIGOP), was unconvincing and was later deemed 'unfit for purpose' (DH, 2015). It was perceived as biased towards the suggested benefits of the initiative, with little information about the opt-out procedure (Vallance, 2014). Patients who decided not to share their data outside the NHS would have had to opt out of sharing information altogether, affecting those who would have liked to participate in research but not in other data uses (Shaw, 2014). The British Medical Association (BMA, 2014) and GPs (Matthews-King, 2014c) insisted that, for this programme of secondary uses beyond direct care, an opt-in approach was more appropriate.

After the Information Governance Review (Department of Health, 2013), NHS England committed to respecting patients' preferences on a statutory basis (Swinford, 2014). Patients could register a type 1 objection if they did not want their data leaving the GP practice or a type 2 objection if they did not want their data leaving the HSCIC in any identifiable form (Roebuck, 2014). It was unclear whether after a type 2 objection a patient could still be approached again for direct care services (e.g., e-referrals).[9] NHS England had never considered the full extent of these concerns which became evident from the fact that it did not initially have the capability to process the growing number of opt outs (Merrick, 2015) and had to work

for over a year to start processing the resulting 1.5 m opt outs (HSCIC, 2016). Moreover, while the HSCIC initially set itself as the only data controller after the extraction of patient records for care.data, in the end, it accepted joint data control with GPs.[10] GPs now had a statutory duty to share this information unless their patients decided otherwise and opted out (Matthews-King, 2014a). These developments also led to the establishment of the role of the National Data Guardian so as to review data sharing and security in the NHS and recommend on more simplified and streamlined opt-out processes (Caldicott, 2016). At the same time, after the public outcry (2014) an advisory group[11] was established by NHS England to help care.data get back on track, in 2016 this group was replaced by a new oversight board.[12] This time, however, privacy campaigners and civil liberties groups were left out of the meetings.

The duty to accept the risk

During the last decade, there have been repeated calls for new laws, information governance policies and ethics procedures for greater, faster and appropriate access to NHS data (Academy of Medical Sciences, 2011). It is believed that the current (complex) situation is too conservative and inclined towards privacy and autonomy at the expense of the public interest (Academy of Medical Sciences, 2006). It instils a fear of litigation across researchers, healthcare professionals and institutions (Clark and Weale, 2011). It slows down and burdens (financially) good research (Academy of Medical Sciences, 2006). For data initiatives, such as care.data, that require the linkage of disparate datasets, complete anonymisation of data would simply render the programme impractical. In this debate between private and public the stakes are clear: too much emphasis on autonomy and privacy risks good research.

On the other hand, risk is also increased due to the centralised nature of the care.data. One central database enjoys economies of scale, but it maximises the susceptibility of datasets to malicious activities. In fact, the number of medical data attacks is growing (ITRC, 2014); for example, 79 million records were compromised at US insurance company Anthem, which shows that sophisticated security systems are often insufficient to safeguard a database (Mathews, 2015). The NHS has become the single largest reporter of data breaches to the ICO (Murphy, 2015). There are also secondary threats from malicious inference from legitimately released data. These cannot be resolved by improved cybersecurity because they only make use of data available legitimately (HSCIC, 2014). While many in the field acknowledge an increased risk of data abuse, they also believe that as long as appropriate measures are in place, such initiatives can be justified (Faden et al., 2013).

Aggregated databases may also produce information beyond a given dataset. Importantly, the simplicity of this record linking and digital processing makes the accuracy of the complete patient record extremely difficult to dispute and may systematically compound social inequalities (Nuffield Council on Bioethics, 2015). A DNA sequence, for example, may reveal information not only about a patient but also about her family (Gertz, 2004), while aggregate genomic data carries a high risk of re-identification (Erlich and Narayanan, 2014). Data mining may lead to profiling with significant social consequences. Existing bio-banks already seek to link their data with records of criminal convictions, earnings and employment data.[13]

HSCIC recognised the operational risks from inappropriate access or imperfect anonymisation of data (Dickinson, 2013). It also accepted the main risk involved in pseudonymisation – the practice of replacing the main patient identifier (i.e. NHS number) with a unique but meaningless pseudonym (Oswald, 2014) – which is the possibility of re-identification of individuals when various datasets are linked together. In response, HSCIC became an '*accredited safe haven*' (DH, 2013) to ensure that such risks are minimised and access restricted to accredited researchers who meet specific criteria (Academy of Medical Sciences, 2011). Importantly, it remained sceptical about pseudonymisation at source (assigning the pseudonym before the extraction) due to the varied healthcare settings and information systems from which data was to be extracted (NHS England, 2014). However, it is working to ensure that any access to pseudonymised, linked, datasets (and any attempts by analysts to re-identify individuals) will be subject to sanction by the ICO (NHS England, 2014). It is unclear whether this is solely for pseudonymised data, since standard and bespoke extracts of personal confidential data are possible at the moment under a data-sharing contract. They just cost more.[14] Despite the fact that literature has ample evidence that demonstrate the limitations of this de-identification mechanism (O'Hara, 2011), central and effective pseudonymisation allows HSCIC to (cost-efficiently) process NHS data outside current data protection regulations and without any particular obligations to the data subjects (ICO, 2012). From there, they can become available for disclosure[15] and processed without always knowing accurately who final data recipients might be.[16]

The duty to assetise

The 2008 global financial crisis, the recession and the prevailing pro-market political-economic approach to public sector administration, as well as the dismantling of the welfare state, have placed the NHS under

immense pressure to close its funding gap. From the Wanless Report to the 'Nicholson Challenge', successive UK governments have concentrated their efforts on accelerating efficiency gains and productivity improvements, rather than increasing NHS funding out of taxation (Appleby et al., 2014). Simultaneously, the 2012 HSCA epitomised the privatisation of the NHS via the contracting of NHS services to private providers (Pollock, 2015). With personal data being termed as the new asset (Schwab et al., 2011) in this post-industrial information era and its economic value amounting to a new kind of equity (Mohamed and Ismail, 2012) for organisations and businesses to increase their capital, NHS data is also seen as a valuable source of income for the sustainability of the NHS (see George Freeman, 2010; Martin and Hollin, 2014).

Actors from the wider public and private sectors, including the pharmaceutical and insurance industries, have always been interested in getting access to NHS data (Tiner, 2007). HSCIC was (before the public outcry) able to tailor its data service to these potential customers' needs (McKinsey & Company, 2014). The purpose has not been to make a direct profit out of the selling of these data assets – any associated fees are usually there to cover the costs of dataset preparation and the auditing and managing of the contracts. It is more about facilitating data sharing among actors within the wider economy that can exploit them for knowledge and profit (Schwab et al., 2011). For example, the Institute and Faculty of Actuaries (IFoA) purchased all HES records between 1997 and 2010 combined with credit ratings and deprivation (IFoA, 2014). While it is unclear from the published report how the datasets were linked and by whom, its researchers were able to advise the health insurance sector on pricing practices for first incidences of critical illnesses by using geodemographic profiling from actual (individual-level and anonymised) data rather 'relying on approximations' (IFoA, 2014: 9). Interest is also growing from other government departments, such as the Department of Work and Pensions (Baldwin, 2014), the Police and the National Crime Agency. The Partridge Data Review (HSCIC, 2014) was particularly illuminating. More than half of data releases (from the sample studied) were made to various private sector organisations under a rather dubious information governance framework (HSCIC, 2014). HSCIC had subsequently to change its contract policy and become more transparent by developing a basic register with data access contracts.[17]

Despite the fact that several surveys have shown that the public does not trust commercial companies with their data, whether legitimately accessed or not (Clemence et al., 2013; Wellcome Trust, 2013), and would not like to see their data being shared solely for commercial gain (Hill et al., 2013; Wellcome Trust, 2013), the updated legislative framework (Care Act 2014, 2014) still does not draw distinctions between the private and the public sector when it comes to data access requests. While it emphasises respect for patients' privacy by HSCIC (section 253), profit-making is not strictly prohibited. Therefore, any organisation can request, receive and analyse NHS data as long as it can justify that the information will be used for the provision of services and the promotion of health (section 261). For example, a pharmaceutical company can request data to study, for 'public benefit', the efficacy of a drug even if the company benefits financially as well. The current regulatory and technical framework appears '*to want to keep the scope of potential uses broad, in the spirit of treating data as a resource with multiple and undefined potential uses*' (Nuffield Council on Bioethics, 2015: 112). However, this is to be expected. Understanding data accumulation in market terms, listing all potential secondary (re-)uses to citizens for informed decision-making is impossible. An omnibus information provider always has to plan ahead and continuously prepare for future, yet to be identified, data collection requirements and uses (Andrejevic, 2013). In healthcare, a viable return on investment can only be generated by the multiple use of datasets produced from large-scale, accelerated and inexpensive studies (Gaye et al., 2014). This is why, when it comes to data sharing initiatives and secondary uses, 'notice and consent' is treated as being impractical (Mayer-Schönberger and Cukier, 2013). That is why data cannot be conceived as a commodity but more of an asset ready to be deployed, according to market directions.

Conclusions

In this paper, we used the framework of CI to offer an alternative reading of the care.data conundrum by avoiding the dichotomy between what is public and private health data. We focused not only on the new systems, legal and policy frameworks establishing new information flows and transmission principles, but also on identifying actors and processes that attempt to erode the public healthcare sector while privileging new information recipients. Care.data can be understood as an attempt by the state to place itself as the new, central, data broker (Keen et al., 2013) by establishing those information flows and transmission principles that would facilitate the assetisation of NHS datasets for the financialisation of the knowledge economy (Lazzarato, 2009). After any 'ownership' rights had been reappropriated, these datasets would have been re-contextualised and rented to actors in other parts of the scientific and economic industries to extract

surplus value. However, this process has proved not to be that straightforward. NHS datasets do not hold only one (monetary) value, but a range of other scientific, social and ethical *values* (Birch and Tyfield, 2013) that often determine the fate of their assetisation.

From a CI perspective, patients, as data subjects, provide (personal confidential) – and hard to alter if something goes wrong – information about symptoms they experience to their GP who then receives and records this for patient management. After GPs, HSCIC is the second-stage recipient of this longitudinal information that processes this data for all sorts of analyses related to the operation and financing of the NHS. The original aspirations of care.data and the data disclosure to IFoA – before data extractions for care.data even started – can be understood as 'evidence of a clash of contexts' (Nissenbaum, 2010: 225). It alerted parts of the society that the context of the NHS is changing beyond that which was originally agreed.

Undoubtedly, confidentiality, reciprocity and autonomy, with regards to notice and consent, are fundamental principles in the healthcare and academic research contexts. Patients still expect that they can trust GPs with their information and that GPs are capable of making good use of it to treat *them* as well as *others*, with a certain level of transparency and accountability. Patients also appear to strongly maintain their rights and engage with decision-making processes about secondary uses. The new context of information sharing that care.data and the new regulations initially implied was that patients should also contribute data for the country's economic prosperity, in the widest and most ambiguous sense of the term. This new, economically narrowed, value caused care.data to be perceived as a threat to a long established social licence for research within the NHS and healthcare, particularly around issues of trust, the new obligations of GPs in their relationship with patients and NHS patient data as a public good (Carter et al., 2015). It signalled that a new kind of social contract of shared investment and risk between patients and the NHS is in the making (Carter et al., 2015). It showed that there are now (unknown) actors outside the NHS that want to become new recipients of *patients*' data, free and without patients' and GPs' having the opportunity to express an opinion. The attempted mandatory patient data extractions across the NHS, without a choice for GPs and patients, led care.data to be seen as a paternalistic and hurried process of 'conscription' (Sterckx et al., 2015). When patients became aware of the endless possibilities that could open up from combining these healthcare datasets with other datasets from other industries, they also became aware of the potential misuses of this data. Various public and private actors were already working to develop the technical and legal frameworks for secondary uses before this programme was ever brought to the public and GPs for consultation.

In a recent report by Ipsos MORI for the Wellcome Trust (Castell and Evans, 2016), researchers came to similar conclusions and talked about '*context collapse*' as way to explain how the realisation of health data being used in commercial contexts confuses the public and makes it suspicious, as well as protective of their data. They concluded that, a clear public benefit and some kind of consent (for any kind of research) had to be demonstrated and provided before the public becomes comfortable with sharing their data. Insurance and marketing, and, to a certain extent, pharmaceutical, companies were not seen as appropriate data recipients. Trust in new information flows was also largely linked to transparency and accountability.

Reaction to care.data seems to be based on the understanding that NHS data, coming from a network of organisations funded by the public for supporting the healthcare of all citizens, is a public good and should not engage in market exchanges. The exchange of information within the healthcare context takes place on a voluntary and consensual way. In the commercial context it takes place according to the rules of the market. While the former context is there to support health, the latter is there to support capital accumulation. Therefore, profit-making on this data is seen as an end contrary to the goals of the NHS. Disclosure of NHS data to actors and industries that have not traditionally been part of (publicly funded) healthcare, and are not expected to give something back to the NHS, will be treated as problematic and are likely to be highly resisted. Private insurance and marketing industries will experience resistance, as not only are they motivated by profit, but they are also not expected to reciprocally improve the NHS or contribute to its sustainability. Their business is about providing highly differentiated products and services to a small number of individual customers who can afford them and is predicated on excluding potential customers on the basis of their health conditions. Pharmaceutical companies, while they are expected to give something back to the NHS (e.g., drugs) from their analyses of NHS data, are perceived to have done this at a great cost to the service. Profit-making in conjunction with discriminatory or disadvantageous (for the public and the NHS) use of NHS data will probably be strongly contested.

Moreover, we already mentioned a number of not-for-profit academic and governmental databases that facilitate healthcare research, but compared to care.data they have different transmission principles. They collect data from GP practices through practices opting in and patients can exercise one simple opt out.

Academic healthcare research is founded on certain principles, strongly endorsed by the public: transparency, accountability and scientific scrutiny. While there is still a lot of work to be done, researchers are actively calling for further development of these principles, for example via the release of datasets, study protocols (Iqbal et al., 2016) and the analytic codes used (Goldacre, 2016).

Undoubtedly, the NHS has entered the new informational era and aspires to lead the way in digital health. It makes increasing use of EHR data and it is strategically exploring opportunities in consumer health informatics, for example, via the provision of free devices and apps to patients so as to instil personal engagement and accountability in the prevention, self-care and management of patients' illnesses (Campbell, 2016). However, while people *choose* to join an online social network or buy a wearable device for better, faster and more personalised services this does not mean that they will always *have* to agree to every new information flow and that their data is up for grabs and exploitation. Parts of the user community are always on alert to protest against new information flows that violate their expectations of privacy (Fletcher, 2010) and how other actors are trying to profit out of the unpaid and affective '*immaterial labour*' (Terranova, 2000) they have put in to feed the platform with their data. As the public's awareness of such issues and practices increases so will its sense of privacy violations (Nissenbaum, 2010).

Therefore, the conundrum, particularly in healthcare and around care.data, is not just about privacy versus openness (Vayena and Gasser, 2016). Such dichotomous approaches tend to substitute political, economic and ethical discussions for organisational processes, computational frameworks of security and appropriate de-identification methodologies. By concentrating discussions on the (im-)practicability of consent, other, *equally* important issues are left out: who ought to have access to data, for what (dis)advantageous purposes and what are the financial issues at stake.

Based on the four duties (to share, to not opt out, to accept the risk, to assetise) we identified here, we can argue that non-egalitarian and unprincipled approaches to autonomy and reciprocity may backfire and foster resistance that may render such data sharing initiatives useless in practice. As the patient–clinician relationship gets jeopardised due to the lack of trust around protection of sensitive data from market-driven exploitation and discriminatory practices, more people may avoid GPs, delay appointments, withhold crucial health information or even provide false information to their clinician (Clark and Weale, 2011). We may see more patients avoiding healthcare research and opting out of these databases. This will affect the accuracy and completeness of EHRs (NHS England, 2014), creating biased datasets (Pollock and Roderick, 2014).

As care.data amply demonstrated, there is a new policy direction that aims at constituting sustainability, governance and economic growth as the de facto social values, while reducing privacy (as a reassurance of trust, exercise of choice and protection from exploitation) to an individualistic preference (Nuffield Council on Bioethics, 2012). It subtly implies that it would be individuals, rather than organisations or public institutions, who will be forced to deal personally with the healthcare, social and financial consequences of ever-increasing and ambiguous data dissemination practices (Rössler, 2005) among entities they are not always aware of. If successful, an economic rationality and governmentality (McNay, 2009), founded on a transactional understanding of potential benefits and rights, risks and rewards in healthcare, will gradually prevail. The integrity of public healthcare will be compromised, nurturing more healthcare and informational challenges for it.

Therefore, for such initiatives to succeed, the aforementioned principles, such as transparency, accountability, (socio-)scientific scrutiny, need to be reinforced judicially so as to effect those information flows and data uses that support patients' equal knowledge of the actors, workings and flows of their sensitive health information (Kelly et al., 2015). Otherwise, the next conundrum in healthcare will focus on how actors and processes of the new healthcare context (with regards to principles and information flows) may risk good health services (Nissenbaum, 2010) and the preservation of the NHS as the fundamental pillar of the collective health of the nation. We should always be reminded that all this wealth of digitised public health data is now available for various kinds of research and for the greater good not only because of the recent computational, scientific and clinical advances in data processing and analysis, but also because of long-standing principles and fundamental *rights*, guaranteed to every individual member of the public, exercised securely and autonomously across multiple contexts (Dawes, 2011) within society.

Declaration of conflicting interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) disclosed receipt of the following financial support for the research, authorship, and/or publication of this article: Paraskevas Vezyridis is supported by a Marie Skłodowska-Curie Individual Fellowship from European Commission (2014-IF-659478). Stephen Timmons is partially

supported by the National Institute for Health Research (NIHR) Collaboration for Leadership in Applied Health Research and Care (East Midlands). The views expressed are those of the authors and not necessarily those of the EC, NHS, the NIHR or the Department of Health.

Notes

1. https://www.england.nhs.uk/ourwork/tsd/care-data/.
2. http://www.hscic.gov.uk/media/15110/Benefits-plan—caredata-updated-addendum/pdf/Benefits_plan_-_care.data_addendum_v2.0.pdf.
3. https://www.england.nhs.uk/2014/02/19/response-info-share/.
4. www.qresearch.org; www.researchone.org; www.cprd.com.
5. http://www.hra.nhs.uk/about-the-hra/our-committees/section-251/what-is-section-251/.
6. http://www.hscic.gov.uk/media/15110/Benefits-plan—caredata-updated-addendum/pdf/Benefits_plan_-_care.data_addendum_v2.0.pdf.
7. https://ico.org.uk/for-organisations/guide-to-data-protection/key-definitions/.
8. https://web.archive.org/web/20140810130424/http://www.england.nhs.uk/wp-content/uploads/2014/03/cd-gp-faq-03-14.pdf.
9. http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/health-committee/handling-of-nhs-patient-data/written/17671.html.
10. https://www.england.nhs.uk/2014/02/19/response-info-share/.
11. http://www.parliament.uk/business/publications/written-questions-answers-statements/written-question/Lords/2015-12-15/HL4600/.
12. http://www.parliament.uk/business/publications/written-questions-answers-statements/written-question/Lords/2016-01-20/HL5266/.
13. http://www.bristol.ac.uk/alspac/researchers/resources-available/data-details/linkage/.
14. http://www.hscic.gov.uk/media/14839/DARS—Service-charges/pdf/dles_service_charges__2015_16_V10_050913_WIP.pdf.
15. https://www.whatdotheyknow.com/request/review_of_pseudonymisation_at_so#incoming-496410.
16. See Q272 at http://data.parliament.uk/writtenevidence/WrittenEvidence.svc/EvidenceHtml/8416.
17. www.hscic.gov.uk/dataregister.

References

Academy of Medical Sciences (2006) *Personal Data for Public Good: Using Health Information in Medical Research: A Report*. London: Academy of Medical Sciences.

Academy of Medical Sciences (2011) *A New Pathway for the Regulation and Governance of Health Research/Academy of Medical Sciences*. London: Academy of Medical Sciences.

Andrejevic M (2013) *Infoglut: How Too Much Information Is Changing the Way We Think and Know*. New York, NY: Routledge.

Appleby J, Galea A and Murray M (2014) *The NHS Productivity Challenge: Experience from the Front Line*. London: King's Fund.

Baldwin C (2014) NHS England admits failure to explain benefits of care.data. *ComputerWeekly*. Available at: http://www.computerweekly.com/news/2240215074/NHS-England-admits-failure-to-explain-benefits-of-caredata (accessed 7 December 2015).

Berry JG, Ryan P, Gold MS, et al. (2012) A randomised controlled trial to compare opt-in and opt-out parental consent for childhood vaccine safety surveillance using data linkage. *Journal of Medical Ethics* 38(10): 619–625.

BIGT (2003) *Bioscience 2015: Improving national health, increasing national wealth*. Report of the Bioscience Innovation and Growth Team. London: Department of Trade and Industry.

Birch K and Tyfield D (2013) Theorizing the bioeconomy: Biovalue, biocapital, bioeconomics or . . . what? *Science, Technology and Human Values* 38(3): 299–327.

BMA (2014) Patients' medical data sacrosanct, declares BMA. *BMA*. Available at: http://bma.org.uk/news-views-analysis/news/2014/june/patients-medical-data-sacrosanct-declares–bma (accessed 15 October 2015).

Bosanquet N and Evans E (2014) *Sustaining Universal Healthcare in the UK: Making Better Use of Information*. London: Volterra Partners.

Brown I, Brown L and Korff D (2010) Using NHS patient data for research without consent. *Law, Innovation and Technology* 2(2): 219–258.

Busby H and Martin P (2006) Biobanks, national identity and imagined communities: The case of UK biobank. *Science as Culture* 15(3): 237–251.

Caldicott DF (2016) Review of data security, consent and opt-outs. *National Data Guardian for Health and Care*. Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/535024/data-security-review.PDF (accessed 7 July 2016).

Campbell D (2016) NHS to offer free devices and apps to help people manage illnesses. *The Guardian*. Available at: https://www.theguardian.com/society/2016/jun/17/nhs-to-offer-free-devices-and-apps-to-help-people-manage-illnesses (accessed 7 July 2016).

Care Act 2014 (2014) Available at: http://www.legislation.gov.uk/ukpga/2014/23/contents/enacted/data.htm (accessed 4 June 2016).

Carter P, Laurie GT and Dixon-Woods M (2015) The social licence for research: Why care.data ran into trouble. *Journal of Medical Ethics* 41(5): 404–409.

Castell S and Evans H (2016) *The one-way mirror: Public attitudes to commercial access to health data*. Report prepared for the Wellcome Trust. London: Ipsos MORI Social Research Institute.

Chan S and Harris J (2009) Free riders and pious sons – Why science research remains obligatory. *Bioethics* 23(3): 161–171.

Clark S and Weale A (2011) *Information Governance in Health: An Analysis of the Social Values Involved in Data Linkage Studies*. London: Nuffield Trust.

Clemence M, Gilby N, Shah J, et al. (2013) *Wellcome Trust Monitor Wave 2: Tracking Public Views on Science,*

Biomedical Research and Science Education. London: Research, Ipsos Mori.

Cooper M (2008) *Life as Surplus: Biotechnology and Capitalism in the Neoliberal Era (In vivo)*. Seattle: University of Washington Press.

Davies G, Frow E and Leonelli S (2013) Bigger, faster, better? Rhetorics and practices of large-scale research in contemporary bioscience. *BioSocieties* 8(4): 386–396.

Dawes S (2011) Privacy and the public/private dichotomy. *Thesis Eleven* 107(1): 115–124.

Department of Health (2002) *Health Service (Control of Patient Information) Regulations 2002*. London: The Stationery Office.

Department of Health (2011) *Innovation Health and Wealth, Accelerating Adoption and Diffusion in the NHS*. London: Crown.

Department of Health (2012a) *Health and Social Care Act 2012*. London: The Stationery Office.

Department of Health (2012b) *The Power of Information: Putting All of Us in Control of the Health and Care Information We Need*. London: Crown.

Department of Health (2013) *Information: To Share or Not to Share? The Information Governance Review*. London: Department of Health.

Department of Health (2015) *Information: To Share or Not to Share – The Independent Information Governance Oversight Panel's report to the Secretary of State for Health*. London: Crown.

Dickinson A (2013) *Privacy Impact Assessment; Functions of the Health and Social Care Information Centre*. Leeds: Health and Social Care Information Centre.

Dixon-Woods M, Ashcroft RE, Jackson CJ, et al. (2007) Beyond 'misunderstanding': Written information and decisions about taking part in a genetic epidemiology study. *Social Science and Medicine* 65(11): 2212–2222.

Dixon-Woods M and Tarrant C (2009) Why do people cooperate with medical research? Findings from three studies. *Social Science and Medicine* 68(12): 2215–2222.

Donnelly L (2014) Hospital records of all NHS patients sold to insurers. *The Telegraph*, 23 February. Available at: http://www.telegraph.co.uk/news/health/news/10656893/Hospital-records-of-all-NHS-patients-sold-to-insurers.html (accessed 15 October 2015).

Erlich Y and Narayanan A (2014) Routes for breaching and protecting genetic privacy. *Nature Reviews Genetics* 15(6): 409–421.

Faden RR, Kass NE, Goodman SN, et al. (2013) An ethics framework for a learning health care system: A departure from traditional research ethics and clinical ethics. *Hastings Center Report* 43: S16–S27.

Fletcher D (2010) How facebook is redefining privacy. *TIME*. Available at: http://content.time.com/time/magazine/article/0,9171,1990798,00.html (accessed 30 October 2015).

Freeman G (2010) House of commons debates: Policy for growth, 11 November 2010. Available at: http://www.publications.parliament.uk/pa/cm201011/cmhansrd/cm101111/debtext/101111-0003.htm#10111155001605 (accessed 25 June 2016).

Freeman G (2016) Review of health and care data security and consent. Available at: https://www.gov.uk/government/speeches/review-of-health-and-care-data-security-and-consent (accessed 7 July 2016).

Gaye A, Marcon Y, Isaeva J, et al. (2014) DataSHIELD: Taking the analysis to the data, not the data to the analysis. *International Journal of Epidemiology* 43(6): 1929–1944.

Gertz R (2004) Is it 'me' or 'we'? Genetic relations and the meaning of 'personal data' under the data protection directive. *European Journal of Health Law* 11(3): 231–244.

Goldacre B (2016) The BMJ should require all papers to share their analytic code. *BMJ*. Available at: http://www.bmj.com/content/351/bmj.h4596/rr-55 (accessed 15 January 2016).

Grace J and Taylor MJ (2013) Disclosure of confidential patient information and the duty to consult: The role of the health and social care information centre. *Medical Law Review* 21(3): 415–447.

Health Information and Quality Authority (2014) *International Review of Approaches Countries Have Taken to Integrate National Health and Social Care Data Collections*. Dublin: HIQA.

Hill EM, Turner EL, Martin RM, et al. (2013) 'Let's get the best quality research we can': Public awareness and acceptance of consent to use existing data in health research: a systematic review and qualitative study. *BMC Medical Research Methodology* 13: 72.

HITF (2004) *Better health through partnership: A programme for action*. Final Report by the Healthcare Industries Task Force. London: Crown.

HM Government (2011) PM speech on life sciences and opening up the NHS. Available at: https://www.gov.uk/government/speeches/pm-speech-on-life-sciences-and-opening-up-the-nhs (accessed 4 June 2016).

HM Government (2012) *Open Data White Paper: Unleashing the Potential*. London: Stationery Office.

Hoeksma J (2014) The NHS's care.data scheme: What are the risks to privacy? *BMJ* 348: g1547–g1547.

House of Commons (2014) Health committee. Oral evidence: Handling of NHS patient data [HC 1105] (8 April 2014). Available at: http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/health-committee/handling-of-nhs-patient-data/oral/8416.html (accessed 4 June 2016).

HSCIC (2014) *Data Release Review*. Leeds: Health and Social Care Information Centre.

HSCIC (2016) Care information choices – April 2016. Available at: http://www.hscic.gov.uk/catalogue/PUB20527/exp-care-info-choi-eng-ccg-apr-2016.pdf (accessed 25 April 2016).

Information Commissioner's Office (2012) *Anonymisation: Managing Data Protection Risk Code of Practice*. Cheshire, UK: ICO.

Institute and Faculty of Actuaries (2014) Telegraph article rebuttal. *Institute and Faculty of Actuaries (IFoA)*, 25 February. Available at: https://www.actuaries.org.uk/news-and-insights/media-centre/media-releases-and-statements/telegraph-article-rebuttal (accessed 15 October 2015).

Iqbal SA, Wallach JD, Khoury MJ, et al. (2016) Reproducible research practices and transparency across the biomedical literature. *PLoS Biology* 14(1): e1002333.

ITRC (2014) *Data Breach Reports*. San Diego, CA: Identity Theft Resource Center.

Keen J, Calinescu R, Paige R, et al. (2013) Big data + politics = open data: The case of health care data in England: The case of health care data in England. *Policy and Internet* 5(2): 228–243.

Kelly SE, Spector TD, Cherkas LF, et al. (2015) Evaluating the consent preferences of UK research volunteers for genetic and clinical studies. *PLoS One* 10(3): e0118027.

Laurie G (2009) Role of the UK biobank ethics and governance council. *The Lancet* 374(9702): 1676.

Lazzarato M (2009) Neoliberalism in action: Inequality, insecurity and the reconstitution of the social. *Theory, Culture and Society* 26(6): 109–133.

Lezaun J and Montgomery CM (2015) The pharmaceutical commons: Sharing and exclusion in global health drug development. *Science, Technology and Human Values* 40(1): 3–29.

McKinsey & Company (2014) Care.data: Turning data into insights. Discussion document, Health and Social Care Information Centre. Available at: http://www.hscic.gov.uk/media/16021/Caredata-and-McKinsey/pdf/Care.data_and_McKinsey.pdf (accessed 15 October 2015).

Macleod U and Watt GCM (2008) The impact of consent on observational research: A comparison of outcomes from consenters and non consenters to an observational study. *BMC Medical Research Methodology* 8: 15.

McNay L (2009) Self as enterprise: Dilemmas of control and resistance in Foucault's the birth of biopolitics. *Theory, Culture and Society* 26(6): 55–77.

Martin P and Hollin G (2014) A new model of innovation in biomedicine? Available at: http://nuffieldbioethics.org/wp-content/uploads/A-New-Model-of-Innovation_web.pdf (accessed 15 October 2015).

Mathews AW (2015) Anthem: Hacked database included 78.8 million people. *The Wall Street Journal*. Available at: http://www.wsj.com/articles/anthem-hacked-database-included-78-8-million-people-1424807364 (accessed 15 October 2015).

Matthews-King A (2014a) GP hit with contract notice over plan to opt all patients out of care.data. *Pulse Today*. Available at: http://www.pulsetoday.co.uk/your-practice/practice-topics/it/gp-hit-with-contract-notice-over-plan-to-opt-all-patients-out-of-caredata/20005749.article#.VVILUNOqqkp (accessed 10 May 2015).

Matthews-King A (2014b) GPs held responsible for patient complaints over NHS data-sharing project, says ICO. *Pulse Today*. Available at: http://www.pulsetoday.co.uk/your-practice/practice-topics/it/gps-held-responsible-for-patient-complaints-over-nhs-data-sharing-project-says-ico/20005505.article#.VVIgHdOqqko (accessed 10 May 2015).

Matthews-King A (2014c) GPs vote in favour of an opt-in system for care.data. *Pulse*. Available at: http://www.pulsetoday.co.uk/your-practice/practice-topics/it/gps-vote-in-favour-of-an-opt-in-system-for-caredata/20006796.article#.VXqMYhNsFBd (accessed 15 October 2015).

Mayer-Schönberger V and Cukier K (2013) *Big data: a revolution that will transform how we live, work and think*. London: Murray.

Merrick R (2015) NHS fails to cope with care.data opt outs. *UKAuthority.com*. Available at: http://www.ukauthority.com/news/5412/nhs-fails-to-cope-with-caredata-opt-outs (accessed 15 October 2015).

Mohamed S and Ismail O (2012) *Data Equity: Unlocking the Value of Big Data*. London: Centre for Economics and Business Research.

Murphy M (2015) NHS tops the list for serious data breaches last year. *ComputerWorldUK*. Available at: http://www.computerworlduk.com/security/nhs-tops-list-for-serious-data-breaches-last-year-3607138/ (accessed 10 May 2015).

National Audit Office (2015) General practice extraction service – Investigation. Report by the Comptroller and Auditor General. Available at: http://www.nao.org.uk/wp-content/uploads/2015/07/General-Practice-Extraction-Service-Investigation.pdf (accessed 10 December 2015).

NHS England (2014) *Privacy Impact Assessment: Care.Data*. Available at: https://www.england.nhs.uk/wp-content/uploads/2014/04/cd-pia.pdf (accessed 5 October 2015).

Nissenbaum H (2010) *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford, CA: Stanford Law Books.

Nissenbaum H (2011) A contextual approach to privacy online. *Daedalus* 140(4): 32–48.

Nuffield Council on Bioethics (2012) *Emerging Biotechnologies: Technology, Choice and the Public Good*. London, UK: Nuffield Council on Bioethics.

Nuffield Council on Bioethics (2015) *The Collection, Linking and Use of Data in Biomedical Research and Health Care: Ethical Issues*. London, UK: Nuffield Council on Bioethics.

O'Hara K (2011) *Transparent Government, Not Transparent Citizens: A Report on Privacy and Transparency for the Cabinet Office*. Southampton: University of Southampton.

Oswald M (2014) *Information Governance Assessment*. Leeds: Health and Social Care Information Centre.

Pathak J, Kho AN and Denny JC (2013) Electronic health records-driven phenotyping: Challenges, recent advances, and perspectives. *Journal of the American Medical Informatics Association* 20(e2): e206–e211.

Perera G, Holbrook A, Thabane L, et al. (2011) Views on health information sharing and privacy from primary care practices using electronic medical records. *International Journal of Medical Informatics* 80(2): 94–101.

Pollock AM (2015) Will politicians be architects or destroyers of the NHS? *The Lancet* 385(9974): 1171–1172.

Pollock AM and Roderick P (2014) Trust in the time of markets: Protecting patient information. *Lancet* 383(9928): 1523–1524.

Rajan KS and Leonelli S (2013) Introduction: Biomedical trans-actions, postgenomics, and knowledge/value. *Public Culture* 25(371): 463–475.

Ridgeway JL, Han LC, Olson JE, et al. (2013) Potential bias in the bank: What distinguishes refusers, nonresponders and participants in a clinic-based biobank? *Public Health Genomics* 16(3): 118–126.

Roebuck C (2014) *HSCIC Data Pseudonymisation Review – Interim Report*. Leeds: Health and Social Care Information Centre.

Rössler B (2005) *The Value of Privacy*. Cambridge: Polity Press.

Schwab K, Marcus A, Oyola JO, et al. (2011) *Personal Data: The Emergence of a New Asset Class*. Geneva: World Economic Forum.

Shaw D (2014) Care.data, consent, and confidentiality. *Lancet* 383(9924): 1205.

Singleton P and Wadsworth M (2006) Consent for the use of personal medical data in research. *BMJ* 333(7561): 255–258.

Sterckx S, Rakic V, Cockbain J, et al. (2015) ''You hoped we would sleep walk into accepting the collection of our data'': Controversies surrounding the UK care.data scheme and their wider relevance for biomedical research. *Medicine, Health Care and Philosophy* 19(2): 177–190.

Swinford S (2014) NHS legally barred from selling patient data for commercial use. *The Telegraph*. Available at: http://www.telegraph.co.uk/news/health/10669295/NHS-legally-barred-from-selling-patient-data-for-commercial-use.html (accessed 10 May 2015).

Taylor M (2014) Information governance as a force for good? Lessons to be learnt from care.data. *SCRIPTed* 11(1). Available at: http://script-ed.org/?p = 1377.

Terranova T (2000) Free labor: Producing culture for the digital economy. *Social Text* 18(2): 33–58.

Tiner R (2007) House of Commons Health Committee: The Electronic Patient Record. Written evidence submitted by the Association of the British Pharmaceutical Industry [HC 422-II]. London: The Stationery Office. Available at: http://www.publications.parliament.uk/pa/cm200607/cmselect/cmhealth/422/422ii.pdf (accessed 4 June 2016).

Torjesen I (2014) NHS England postpones roll-out of care.data programme by six months. *BMJ* 348: g1689–g1689.

Triggle N (2014) Care.data: How did it go so wrong? *BBC News*. Available at: http://www.bbc.co.uk/news/health-26259101 (accessed 15 October 2015).

Vallance C (2014) Adults 'unaware of NHS data plans'. *BBC News*. Available at: http://www.bbc.co.uk/news/health-26187980 (accessed 15 October 2015).

Vayena E and Gasser U (2016) Between openness and privacy in genomics. *PLoS Medicine* 13(1): e1001937.

Verhulst S, Noveck B, Caplan R, et al. (2014) *The Open Data Era in Health and Social Care*. New York: The GOVLAB (NYU).

Wellcome Trust (2013) *Summary Report of Qualitative Research into Public Attitudes to Personal Data and Linking Personal Data*. London, UK: Wellcome Trust.

Willison DJ, Keshavjee K, Nair K, et al. (2003) Patients' consent preferences for research uses of information in electronic medical records: Interview and survey data. *BMJ* 326(7385): 373.