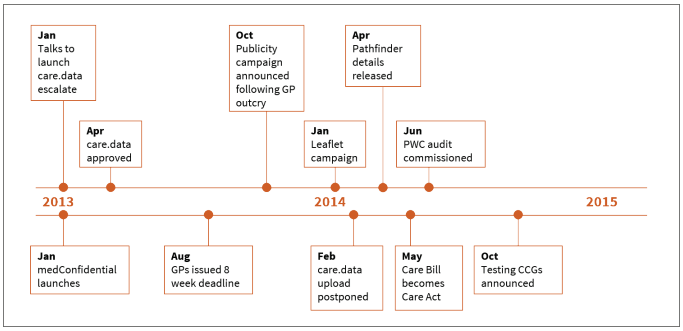
Presser L, Hruskova M, Rowbottom H, Kancir J. Care.data and access to UK health records: patient privacy and public trust. *Technology Science*. 2015081103. August 11, 2015. http://techscience.org/a/2015081103

Care.data and access to UK health records: patient privacy and public trust

Lizzie Presser, Maia Hruskova, Helen Rowbottom, and Jesse Kancir

Highlights

- In 2013, the United Kingdom launched care.data, an NHS England initiative to centralize patient health and social care data.
- care.data faces multiple challenges due to its mismanagement and miscommunications, inadequate protections for patient anonymity, and conflicts with doctors
- Lessons from the care.data experience show the need for clear communications to the public, easy-to-understand consent rules, and strong oversight over purchases of patient data



UK care.data Timeline

Abstract

In 2013, the United Kingdom launched care.data, an NHS England initiative to combine patient records, stored in the machines of general practitioners (GPs), with information from social services and hospitals to make one centralized data archive. One aim of the initiative is to gain a picture of the care being delivered between different parts of the healthcare system and thus identify what is working in health care delivery, and what areas need greater attention and resources. This case study analyzes the complications around the launch of care.data. It explains the historical context of the program and the

controversies that emerged in the course of the rollout. It explores problems in management and communications around the centralization effort, competing views on the safety of "anonymous" and "pseudonymous" health data, and the conflicting legal duties imposed on GPs with the introduction of the 2012 Health and Social Care Act. This paper also explores the power struggles in the battle over care.data and outlines the tensions among various stakeholders, including patients, GPs, the Health and Social Care Information Centre (HSCIC), the government, privacy experts and data purchasers. The predominant public policy question that emerges from this review centers on how best to utilize technological advances and simultaneously strike a balance between the many competing interests around health and personal privacy.

Results summary: Our findings suggest that this balance may be able to be achieved if communication with the public is prioritized, the mechanisms to express consent are specific and easy to understand, control of data is decentralized or centralized only on a small scale, and regulations on purchasers of patient data are clearly outlined and subject to strong government oversight. Our study ultimately finds that the current care.data program is highly problematic in its flawed protection of patient anonymity, an unsuitable opt-out system, unclear criteria for accessing the collected health data, and the risk it poses to the trust between patients and general practitioners.

Introduction

Changes in health policy under the 2010 UK coalition government offer a portrait of active transformation. Notably, the 2012 Health and Social Care Act (HaSCA) broadly reorganized the National Health Service (NHS). As part of these constitutional changes, the revamped Health and Social Care Information Centre (HSCIC) was mandated to collect, hold, and analyze national and personal data; simultaneously, patient information could be legally shared with stakeholders outside of the NHS or medical research community. With this new legislation in place, NHS England's data sharing program, care.data, was created.

Prime Minister David Cameron articulated his vision of data handling in 2011 when he promised forthcoming change. He expressed his government's view that "the end-game is for the NHS to be working hand-in-glove with industry as the fastest adopter of new ideas in the world" [1]. In theory, analysis of centralized and shared data could rapidly transform healthcare provision by linking vast amounts of patient information, analyzing the delivery of specific services and treatments, and ultimately achieving better health outcomes, higher cost savings, and enhanced quality. In practice, the use of centralized health data in British healthcare has been more of a long hurdle race. By early 2014, the care.data centralization effort had spurred a growing public revolt [2]. The program had angered general practitioners (GPs), who were put under unreasonable pressure to notify their patients without ample resources or time. And after NHS England bungled a communications campaign in response, the public cries against the underhanded rollout of the program mounted [2].

Given its potential benefits, how did care.data become so controversial? What critical tensions between government, industry, and the public have been revealed? And what are the future prospects for health data centralization in the UK? This report addresses these questions.

Care.data's Key Complications

This case history investigates the context in which care.data emerged, the process of the launch, and the systemic failures that have been exposed.

Broadly, three problem areas emerge:

1. **Management and Communications:** In the largest overhaul of the centralization of health data, politicians and program managers pushed plans for collecting, storing, and selling national health and social care data without properly consulting stakeholders or informing the general public. As concerns about privacy have grown, the government's response has been insufficient to address public concerns over data safety.

2. **Unrealistic Expectations:** Politicians and program managers categorize data as "anonymous" and "pseudonymous" to assuage concerns about patient identification. But in the technology world, data can rarely be fully anonymous. Data collected for medical research demands certain identifiers that can leave the data vulnerable to re-identification. Also, politicians and the public cannot be expected to sign away data to IT systems that evolve at a rapid pace. A "secure haven for data" today may not be so tomorrow.

3. **Legal Complications:** The care.data program was launched in a contradictory regulatory landscape. GPs are legally torn between their duty to keep their patients' records secure and their duty to transfer records to the Health and Social Care Information Center (HSCIC) for the purpose of "improving patient care." In addition, current statutes and codes applicable to stakeholders are not robust enough to prevent commercial and political actors from using medical data for financial gain.

This Paper by Section

The first section of this paper looks at the historical context of data collection and centralization in the UK, tracking failures from the past. It also looks at the beginnings of "anonymized" data and early privacy concerns. The second section details the proposed mechanics of care.data and the roll-out of the program. It looks at the '"who, "what, "where," and "why" of the program, with a focus on communications around privacy issues. The third section addresses the "when" of care.data and lays out a timeline of key

events. The fourth section sets up the power struggles in the battle over care.data, outlining the tensions between various stakeholders, including patients, GPs, the HSCIC, the government, and purchasers. The fifth section unpacks the legal complexities behind the care.data program and the ways in which various laws demand contradictory duties from certain stakeholders. The sixth section outlines the regulatory landscape and accountability issues that have evolved in response to care.data and its centralization agenda. And the final section looks briefly at the future of care.data.

Background

The history of care.data, proposed in 2012, extends back over a century. In 1911, Prime Minister David Lloyd George introduced the first instance of a data tracking system for GPs that still exists: GP notes on patients stored in manila envelopes [3]. The doctor owned the writing, the Secretary of State owned the paper, and the health record would be handed over to the government for statistical analysis upon a patient's death [4]. In the 1960s, GPs began to log computer records, though the paper envelopes remained mandatory until 2000 [4]. Health records remained in the custody of the particular institution that logged them, and they were neither standardized nor accessible to other healthcare professionals for some time [5].

Hospital Data

The 1980s saw an increase in trust in electronic data over paper records. The NHS began collecting information about every hospital admission across the nation in the form of Hospital Episode Statistics (HES). NHS traditionally stored the information as "anonymous" data. However, information on prescription drugs and test results was absent from this record. Thus, significant gaps in the data existed, and a complete picture of a patient's health could not be constructed. Nonetheless, the NHS claims that HES data was key in the introduction of certain medical advances, such as targeted bowel cancer screening in 2006 [6].

Anonymizing Data

In the 1990s, the NHS identification number was developed. This enabled the "anonymization" of medical records and allowed for the possibility of linking two records held in different locations. This information was added to a national data "spine" that holds demographic data on every English citizen, including name, date of birth, address, and registered GP. The personal spine also includes a summary of clinical conditions and major treatments to "provide anonymous data for public health and health services research." [7]

Precedents to care.data

Anonymization and pseudonymization of patient data at scale was already present in the 1990s with the Hospital Episode Statistics Patient ID (HESID). This is an ID system derived from a number of patient identifiers—such as date of birth, postcode, NHS number, and gender—to help minimize the risk of patient identification [8]. However, the Patient Information Advisory Group (PIAG) voiced concerns over the possibility of patient identification through HESID, and the algorithm was further updated in 2009 to add an additional level of security [8].

The 2000s saw a move to develop a national NHS infrastructure: the NHS National Program for IT (NPfIT). It would be a single repository for healthcare data in England, and it would allow its healthcare data to be used for research and academic analysis in support of the NHS. Initially, the NPfIT, under NHS Connecting for Health, initiated the Secondary Uses Services (SUS), a data warehouse for patient-level information that could be used for research purposes outside of primary care [9]. Although this program was a centralization effort, it did not initially garner mass media attention [10]. In 2003, the NHS Care Records Service proposed a centrally controlled, individual electronic care record (IECR) for all patients in order to connect hospital and GP records and to give healthcare professionals regulated access to electronic health records [11]. By 2006, more than 90 percent of general practices in England were computerized, and one-third held electronic patient medical records [11].

However, the NPfIT system failed for a number of reasons: The top-down approach did not appropriately account for delivery capabilities, politicians did not gain buy-in from key stakeholders, and the rush to delivery involved sidestepping important procurement and legal hurdles [12]. Politicians such as MP Andy Bacon were vocal critics of the program, alongside NHS Trusts, which incurred extremely high costs due to the program [13]. Advocacy groups mobilized against the NPfIT, and NO2ID, a campaigning organization, launched “The Big Opt Out” campaign in 2006, which circulated a widely downloaded opt-out letter [14]. In 2011, the Department of Health announced that NPfIT would be dismantled because “it is no longer appropriate for a centralized authority to make decisions on behalf of local organizations.” [15] The program officially ended in 2013. The failure of NPfIT highlighted the need to meaningfully engage key stakeholders, directly address their interests, and be forthcoming about the values and norms relating to confidentiality of health data [16].

Early Controversies around Centralized Data

In recent years, the NHS’s use of centralized data has drawn much criticism. A 2009 report for Jacob Rowntree ranked the NHS Summary Care Record, which holds information on allergies and current prescriptions of patients, as “amber,” meaning the database had significant problems and may be unlawful. In 2009, one doctor was facing charges for accessing celebrities’ data in Scotland, and the Prime Minister’s data was reported to have been compromised as well [17]. The same report found that the NHS’s Detailed Care

Record ranked "red," meaning the database was "almost certainly illegal under human rights or data protection law." The Detailed Care Record held GP and hospital records in a government-controlled server, and providers could add comments without any professional controls or accountability [17].

As a result of this high-profile report, the coalition government promised to abolish or change NHS systems that might be considered unlawful, and both the Liberals and Conservatives promised to abolish the NHS centralization project if they won in 2010. Instead, once elected, the coalition government simply changed the name of the project and continued to move forward with proposals for data collection [18].

Announcement of care.data

Under the 2012 Health and Social Care Act, the Health and Social Care Information Centre (HSCIC) was modified to collect, transport, store, analyze, and disseminate the nation's health and social care data, continuing the work of the former NHS Information Centre [19]. The Act gave HSCIC the legal and administrative power to collect information on health and social care, securely hold that information, and make the data available for others to use as "actionable business intelligence" [19]. In 2012, NHS England, (initially named the NHS Commissioning Board), was formed under the 2010 coalition government as a special health authority of the NHS "to improve health outcomes of people in England." [20]

In 2013, NHS England (then known as the NHS Commissioning Board) announced plans for care.data, the most recent centralized data initiative. In this program, NHS England could direct the HSCIC to collect health and social care data from all NHS-funded care settings, including information from GP records, and store it in one national database. The data would be stored and maintained by the HSCIC rather than NHS England [21]. It was the first time that GP patient records would exist in a central database, available for medical research by both the NHS and certain private companies. The stated intention was to use the data to assess NHS hospital safety, monitor trends in various diseases and treatments, and plan new health services [22].

Care.data: who, what, where, why

Who: the instigator: Tim Kelsey, the National Director for Patients and Information in NHS England, was the key civil servant who instigated the care.data program. Deeply skeptical of public sector IT projects, Kelsey objected to the inconsistencies in standards of care and the incoherence of access to patient records in public systems. He believed that the private sector had the answer.

In 1999, before he began a career in government, Kelsey founded a private company, Dr. Foster, which monitors hospital performance and mortality rates, analyzes them, and then sells the findings to healthcare organizations including the NHS. The NHS Information

Centre, a public body, controversially bought 50 percent of Dr. Foster in 2006. In 2007, this move came under fire when the National Audit Office voiced concerns over the decision to use public money for the benefit of private shareholders [23].

The merging of public bodies with private interventions has been at the heart of Kelsey's work. Kelsey advocates that big data is fundamental to the sustainability of the NHS and patient health, and he believes in integrating the private sector's practices into the NHS in order to stimulate innovation [24].

What: care.data's proposed structure: NHS England commissioned the care.data service from the HSCIC.

Extracting Information for care.data

The HSCIC extracts data from GP records through the General Practice Extraction Service (GPES) IT system each month. The data includes patient indicators such as date of birth, postcode, NHS number, and gender. The HSCIC can link this data with collected secondary care (hospital data), aggregating it as identifiable, pseudonymous, or anonymous data [25].

What Kind of Data would be Collected?

In the care.data program, the HSCIC collects diagnoses, NHS prescriptions, vaccinations, referrals, and biological values, such as blood pressure, BMI, and cholesterol. But "sensitive" information, such as HIV status, STIs, pregnancy termination, IVF treatment, marital status, complaints, convictions, and abuse, are not to be collected [26]. Handwritten notes are also excluded [27].

Data can be anonymized, identifiable, or pseudonymized, and this process is carried out in accordance with the Information Commissioner's Code of Practice on anonymization:

- **Green data:** anonymous, general data including average values for large groups of patients or other completely anonymous information. This data is aggregated and can be made public.

- **Red data:** personal and confidential data that includes date of birth, NHS number, postcodes, and other identifiers that are vulnerable to identification. HSCIC reports that red data will only be made available in exceptional circumstances, such as in the case of a public health emergency.

- **Amber data:** pseudonymized data at the individual level, which means that patients' identifiers, such as date of birth and postcode, are removed and replaced with a pseudonym. This data can be used to track how individuals interact with different NHS care providers over time. It is possible that this data could be re-identified by companies with access to other data sets. This data is sold only to

> "approved analysts for approved purposes," which can include a variety of research organizations [29].

How is the Data Anonymized or Pseudonymized?

According to those behind care.data, data is anonymized by removing key personal indicators from the records. If anonymized in line with the Information Commissioner's Office (ICO) standards, the data can be freely and safely processed and disclosed. Some data, however, is "pseudonymized," so that it still contains some personal indicators, while other indicators are replaced with pseudonyms. Privacy experts have expressed serious concerns that pseudonymized data can be linked to individuals when it is paired with other information, such as insurance claims, and a report by the HSCIC in 2013 recognized the "risk of malicious re-identification of patients from inference." [28]

Opting in or Opting out

NHS England designed care.data as an "opt-out" program. Secretary State for Health Jeremy Hunt announced that patients would be able to include a code in their records in order to remove their data from the program. Patients could indicate that they did not give permission for their data to be extracted at all or that the data could be extracted but not shared beyond HSCIC. Initially, NHS England announced that GPs would have the responsibility of making patients aware of the opt-out option. Hunt claimed that objections would be respected, except in "special circumstances," as in the case of a civil emergency [29]. Concerns over the opt-out model among GPs, the public, and privacy advocates have risen substantially, and 75% of GPs support a switch to an "opt-in" system. Ross Anderson, professor of security engineering at the University of Cambridge, explains that "the NHS opt-outs are like Facebook's: the defaults are wrong, the privacy mechanisms are obscure, and they get changed whenever too many people learn to use them" [30]. Nonetheless, the program has remained opt-out throughout its history [31].

In addition, opt-out procedures have failed to capture true patient preferences. These failures are detailed below.

Where: a national database: The HSCIC is an executive non-departmental public body that would be the national center for information across health and social care. HSCIC began in 2005 as a trusted safe haven for national health data. It can collect, hold, and release this health data. The HSCIC collects Hospital Episodes Statistics (HES) and accident and emergency information. Through NHS England, this data is then supplemented by primary care data. This combined data is available to certain NHS agencies and can be sold, pending approval, to pharmaceutical companies, health organizations, research universities, hospital trusts, think tanks, and other private companies [32]. The combined data is reserved for secondary use for data, rather than at the point-of-service for patients. According to Guido Van't Noordende, a Dutch health privacy campaigner, centralization of these records on a single, nationwide database involves significant risks. It can only be

effective and safe if the storage, control, and processing functions are decentralized, or, alternatively, if the data is centralized on a regional scale. As such, the responsibilities are less likely to be diluted among the strata of stakeholders (interview with Guido Van't Noordende 2015).

Why: proposed benefits: For the public, proponents of care.data argue that tracking, mining and analyzing the centralized "big data" could help the UK plot patterns of health, better understand diseases, roll out improved treatment regimens, assess health care provider performance, and encourage more effective drug development [33]. They say that sharing of these records could ultimately save lives through sharper investigations of drug side effects, hospital surgical units' performance, and tracking the impacts of drugs and treatments on patients [34].

For the private, in 2014, an HSCIC report revealed that drug companies and insurance companies had been buying information on patients for many years [35]. In addition, news reports revealed that once care.data was live, the newly linked GP and hospital records would be available for sale through the HSCIC as well—including information on mental health conditions, diseases, and unhealthy behaviors [36]. Insurers, drug companies, and other organizations have two routes for accessing data. In the case of care.data, they could apply to HSCIC to gain access to the care.data database, and firms would pay once approved by HSCIC, the Data Access Advisory Group, or the Health Research Authority. Alternatively, private companies could seek patient consent or apply for a legal exemption from consent, such as a Section 251 exemption, as explained below [37].

Methods

We surveyed promotional and academic literature, government reports, and news accounts to document controversies that emerged in the course of the rollout.

Results

This section describes problems observed after the launch of care.data. These included power struggles, a legal debate, and issues of accountability and regulation.

The Launch of Care.data: the roll-out and backlash

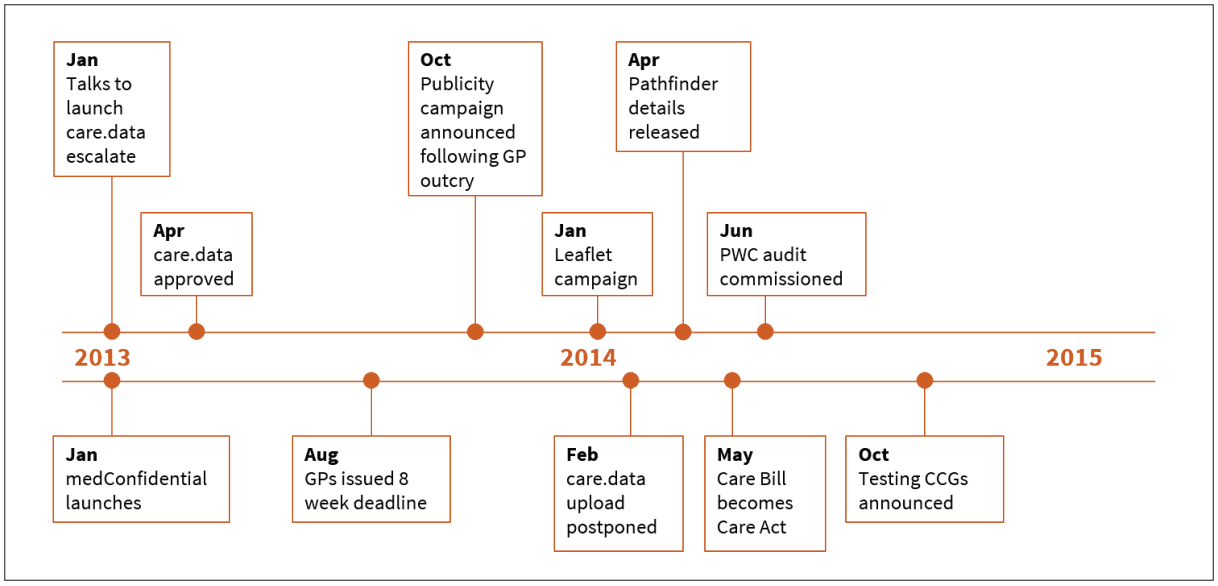


Figure 1. A timeline of events

In January 2013: after NHS England announced plans for care.data, privacy groups including Privacy International, Big Brother Watch, NO2ID, and TheBigOptOut came together with privacy experts such as Terri Dowty, Phil Booth, and others to launch medConfidential, a direct response to the threat of care.data data extraction. This group began a campaign for confidentiality and consent in health and social care to ensure the safety of data sharing.

In April 2013: the GPES Independent Advisory Group approved the extraction of General Practice Extraction Services (GP-level data) as part of the care.data program, and the HSCIC planned to begin extractions in September 2013. Although privacy groups had voiced concerns, the general public was largely unaware of NHS England's plans to centralize GP records. Initially, there was no stated intention to consult or inform the public.

In August 2013: GPs received a letter informing them that they had 8 weeks to notify their patients about the care.data scheme before data extractions began. A GP backlash ensued, as physicians were caught between contradictory obligations. The NHS England and the HSCIC could command data from GPs under Section 259 of the 2012 Health and Social Care Act. Meanwhile, under the Data Protection Act, GPs were obliged to inform patients in a timely manner about opting out if patient information was to be used for a different purpose from that which it was originally collected [38]. A survey of 400 GPs in January 2014 found that 41% would personally opt out of the scheme and 16% were undecided [39]. There was also unreasonable pressure on the GPs to disseminate this information without ample resources [40].

In October 2013: in response to the GP outcry, NHS England announced it would launch a £2m publicity campaign aimed at informing patients of the scheme and their rights.

- Representative committees of NHS GPs, Local Medical Committees (LMCs), considered boycotting the care.data extracts, as they were faced with conflicting legal duties. GPs have a legal duty under the Data Protection Act to protect patient data, and now a statutory obligation through the HaSCA to release the data [41]. LMCs expected that allowing the extracts to occur could make GPs vulnerable to legal action under the Data Protection Act. Not allowing the extracts to occur, however, could be in violation of GPs' statutory obligation as outlined in the Health and Social Care Act (HaSCA). The Information Commissioner, a UK independent authority overseeing data privacy for individuals and transparency from public bodies, also voiced criticism of the program's rollout.

- GPs also pushed back against the government's insistence that it was the responsibility of the GPs to inform patients of the scheme, saying they did not have enough time or funding to do so [41].

In January 2014: a communications disaster began.

- NHS England and HSCIC launched a £2 million public awareness campaign around care.data, sending out a leaflet (costing £1 million) entitled "Better information means better care." There was no cohesive marketing campaign, no national TV campaign, no press conference, and the only supportive media was a video animation posted onto YouTube and the NHS England's website.

- The leaflet communicated an opt-out model, but, crucially, it did not include an opt-out form. Instead, it recommended that patients "speak to (their) GP practice" to opt out or ask further questions.

- The postal service Royal Mail was contracted to reach 99% of households, or 26.5 million homes. The Independent Information Governance Oversight Panel (IIGOP) advised NHS England that the leaflet was not fit for its purpose. But the leaflets had already been sent to the printers, and NHS England did not change course.

- The declared intention was that the leaflets would be plain to see, but the leaflets weren't personally addressed to anyone, and in some cases arrived in households inside junk-food menus. As such, they were discarded as junk mail, or simply weren't received [42]. A BBC poll in February 2014 for Radio 4's PM program, conducted by ICM Research, investigated the impact of leaflets on public awareness [43]. Less than a third of adults (29% of a sample size of 860) recalled ever receiving the leaflet about care.data and the opt-out model [43].

In February 2014: the HSCIC admitted to selling patient data to insurance companies, triggering a more rigorous review of HSCIC data protection [44].

In February 2014: NHS England announced it would postpone uploading GP data onto care.data records for an additional 6 months. Tim Kelsey acknowledged care.data was on the verge of "a crisis in public trust." [45]

- Health data privacy began to make national headlines. In addition to concerns over the HSCIC's data protection, evidence accumulated that the publicity campaign of the NHS, namely leaflets sent to homes in England, failed to appropriately inform the public about the implications of care.data and patients' rights to opt out.

- Jeremy Hunt, the Secretary of State for Health, announced that the government would "unveil new laws to ensure that medical records can only be released when there is a "clear health benefit" rather than for "purely commercial" use by insurers and other companies [46].

- Another source of anger over the opt-out system stemmed from the rigidity of the process and the obscurity of patient choice. Initially, care.data opt out was designed so that once care.data was live, if a patient failed to opt-out pre-launch and his or her medical records were included, the patient would not have the ability to withdraw. Indeed, even if a patient allowed use of their children's records in care.data, those children could not withdraw their data once old enough to decide for themselves [47].

In March 2014: it was reported that certain consultancy groups had access to wide datasets of patient data that could be charted geographically. This led to greater public concern over the protection of data within the HSCIC [48].

In April 2014: the HSCIC released an audit of sales of data in 2013. This audit disclosed that HSCIC had sold anonymous, pseudonymous, and identifiable data to 160 organizations. Following this audit, the public crisis of confidence deepened [49].

In April 2014: Tim Kelsey, NHS England's National Director for Patients and Information, announced that care.data communications pilots, later renamed the "Pathfinder Stage," would be run with between 100 and 500 GP practices [50]. The Pathfinder Stage would test new communications methods to inform the public about care.data, and was due to start in the autumn 2014. The Pathfinder Stage, described as a "last chance saloon" by the *British Medical Journal*, was a phased roll-out to experiment with communication methods for information, safeguards, and data sharing options utilizing selected Clinical Commissioning Groups (CCGs). Methods included further leaflets, addressed letters, emails, and texts from surgeries. Ipsos MORI, a polling agency, was involved in the testing phase [51].

In May 2014: the Care Bill became the Care Act, which provided that health and social data could be shared and analyzed only when there is a "benefit to healthcare," and never for other purposes. In addition, an independent body would scrutinize the use of all the data with transparency.

In June 2014: Sir Nick Partridge, as a non-executive director of the HSCIC, commissioned PriceWaterhouseCoopers to publish a report monitoring all the data released by the NHS Information Centre (NHS IC) since 2005. This audit found "lapses in the strict arrangements that were supposed to be in place to ensure that people's personal data would never be used improperly" [52]. It also found that the HSCIC, and its predecessor, the NHSIC, were responsible for 3,059 data releases that took place between 2005 and 2013. This instigated a public uproar over the HSCIC's lack of transparency over patient privacy [52].

In October 2014: NHS England announced the four CCGs selected for the testing phase: Leeds (the home of NHS England), Somerset (Tim Kelsey's local CCG), West Hampshire, and Blackburn with Darwen, collectively representing 265 GP practices and 2 million patients [53]. There was no transparency as to why these areas had been selected or what methods of analysis would be used in evaluating the success of the pilot. There was no back-up plan if the evidence showed that communication methods were still unsuccessful. No trial start date was set.

Current Status: Where has it Stalled?

In January 2015: it became apparent in a letter [54] submitted to Parliament by the Health and Social Care Information Centre that, owing to a mistake with the "Type 2" (9Nu4) objection code, those who believed they had expressed the preference to opt out would need to re-register their choice for it to count toward care.data. Their opt-out preference covered personal information used in their direct care, rather than the use of their information in secondary care through the care.data program [55].

In February 2015: NHS England's care.data program director Eve Roodhouse declared that the number of patients choosing to opt out of the care.data register would be counted nationally, but not by individual practice and not in an attempt to "beat GPs over the head." [56] An independent care.data review was due in the first trimester of 2015.

In June 2015: the first care.data pilot in Blackburn with Darwen was set to begin. The live trials will begin with NHS England sending an addressed letter to every patient living in the NHS Blackburn with Darwen CCG, and the three other CCGs are set to follow this year. This pilot exercise is expected to involve 104 GP practices by the end of 2015 [57].

The Power Struggle Explained

Medical bodies v. government: Centralized health data highlights well the tension between the state and the medical profession: In order to protect both professional and patient autonomy, physicians have publicly and regularly opposed the UK government's plans to centralize health records.

However, the care.data issue reveals clear internal thought demarcations in the physician community. Consultants and specialists within the British Medical Association (BMA) tend to be more supportive of data centralization, while the General Practitioners Council (GPC) maintains strong opposition [58]. Understanding this divide requires understanding differences in the professional perception of the patient's medical record. Dr. Paul Cundy, long-standing Chair of the IT Committee for the BMA, comments that general practitioners view the medical record as a reflection of their professional relationship with the patient and their status as protectors of the record. The record is sacrosanct, as it may contain biomedical data such as a collection of clinical laboratory values or diagnostic images, but the record also reflects details of the patient's personal life that are non-essential to care [81]. At the heart of this issue is trust: Patients might reconsider their willingness to divulge information to their GP given the requirements of a centralized record and data sharing under Sections 251 and 259 of the 2012 Health and Social Care Act.

In what was widely considered a victory for GPs and patients in July 2014, the Annual Representative Meeting of the BMA (the wider body of all representatives) adopted a motion paralleling the strong anti-centralization position of the GPC that called for halting of care.data because of potential breaches in confidentiality, potential loss of trust, lack of clarity on purpose, commercialization of the data, and the opt-out structure of data collection [81].

Privacy experts v. purchasers: Creating one record that includes the entirety of a patient's medical history, even when pseudonymized, problematically combines enormous data value and great risk, as an entire life record can be traced from one detail. For potential purchasers of a dataset, the larger the dataset, the greater the value for secondary uses. For privacy experts, the larger the dataset, the larger the possibility that the data is re-identifiable.

In March 2014, one month after Health Secretary Jeremy Hunt promised measures were in place to prevent the sale of health data to insurers, *The Guardian* and other news outlets reported that management consultants at PA Consulting had obtained the "entire start-to-finish HES [Hospital Episode Statistics] dataset across all three areas of collection—inpatient, outpatient and A&E." [59] They purportedly had also collected information on location inputs, as they claimed that they could produce interactive maps directly from HES queries. This news arrived after reports that actuaries, pharmaceutical firms, governmental departments, and private health providers had attempted to obtain or succeeded in obtaining patient data as well. This outburst of news alarmed privacy

experts, and patient groups raised concerns over what safeguards were in place. They called for a full disclosure of which organizations had acquired medical records [59].

In April 2014, HSCIC released the first audit of the data disclosures, revealing that medical record information was released to 160 organizations, including 56 private sector organizations [60]. Private healthcare providers, including Bupa, BMI, Care UK, and management consultants, including McKinsey, Ernst & Young, and GE Finnamore, received patient data. The released data was in "pseudonymized" form 347 times, and in identifiable form 75 times. Privacy experts, and in particular, computer scientists, note that data that can be longitudinally charted may not be able to be fully anonymized or pseudonymized [82]. The majority of the identifiable data released by the HSCIC was from HES records [61]. The HSCIC claims it does not profit from the sale of data. The patient privacy group medConfidential alleged that HSCIC omitted key information in this audit that could cause political damage. The HSCIC denies the allegations [61].

Other measures to protect the interests for which we use anonymization and pseudonymization include access control, and legal and ethical safeguards. Access control is a security feature on an operating system that controls who has access to data and resources. This process requires three steps: user identification through a username; authentication, where the user verifies his or her identity through a password or PIN number; and authorization, giving differing degrees of access to the user as determined by pre-set controls [62]. This process is complicated by the complexity of the security technology, the challenge of classifying the information, and the use of the technology [62]. Now, centralized data has created a product of temptingly high value, with penetrable access points—through technology, legal loopholes, and ethical gray areas.

All in all, this debate centers on the ability to protect and maintain the anonymity of patient data, and there are no easy answers. Private sector firms claim that data can be and is truly anonymized, unlinked to individual patients. Many privacy experts do not believe that the current de-identification process can sustainably protect patients. This is a debate being waged in the academic world as well, with law professors, computer scientists and statisticians, among others, grappling with the possibility of re-identification using "anonymized" data.

The public v. HSCIC: When patients do not opt out of care.data uploads, many different stakeholders can gain access to their medical records, ranging from academic researchers to commercial companies, and for different purposes. Among the public, using personal information to develop drugs is perceived favorably, compared to using it to sell people drugs. But the process of buying and accessing data remains opaque. Once a firm submits an application to the HSCIC, the Data Access Advisory Group (DAAG) reviews the application. The DAAG checks that the firm has appropriate mechanisms in place to ensure the safety of the data, and it reviews the stated purpose of the application and the proportionality of the request for data given the stated purpose [64]. However, the criteria

upon which the DAAG judges whether the data will be used for "research" purposes are unclear. Contracts with pharmacies and insurers, for example, have raised eyebrows.

Two major reports made national headlines for identifying regulatory flaws in care.data: The Partridge Review and the Caldicott Report. Both revealed that the data-sharing agreements approved by the HSCIC had been mismanaged. The Partridge Review found that HSCIC and its predecessor, the NHS IC, were responsible for 3,059 data releases that took place between 2005 and 2013. The report does not cover the cost of the data to these companies. However, it did find "lapses in the strict arrangements that were supposed to be in place to ensure that people's personal data would never be used improperly." [65]

Examples include:

- One research program had no legal authority to obtain patient-identifiable data but was still accessing NHS records in 2014.
- "Data sharing agreements" with three reinsurance companies and four pharmaceutical companies including Boots, GSK and AstraZeneca allowed them to use the data until the agreements expired in 2015 and 2016.
- One set of records went to French multinational reinsurer Scor, to the UK subsidiary of the Reinsurance Group of America, and to the reinsurer Millman.

Cambridge University professor of security engineering Ross Anderson explains: "People don't mind Cambridge having their information for medical research, but don't want it to go to Glaxo. They don't realize that Cambridge would have to go to Glaxo to take the medicine to market" [83]. As reports of HSCIC sales of data accumulated and NHS England repeatedly bungled the communications around care.data, the public increasingly voiced concerns over the HSCIC's stated commitment to privacy and made demands for greater safeguards.

The Legal Debate

There is widespread confusion around the legalities of care.data. It stems partly from the fact that in England and Wales the legal basis for sharing medical data is far from clear, as it is difficult to identify a single legal or jurisprudential framework defining such notions as anonymity, privacy, or public health interest [66]. The existence, success, and public acceptance of care.data depend on the legal structure underpinning it as much as on the IT system supporting it.

National and supranational statutes in the UK and EU, together with the binding case law, offer two different interpretations of the legal duty to protect patient data against misuse by public or private actors.

The first interpretation is that data disclosure is only acceptable if the data is altered to such an extent that the information undergoes a "de-identification procedure" through anonymization or pseudonymization [67]. The second interpretation contends that medical data should only be available to "authorized users in circumstances in which they are expected not to harm data subjects," or where users seek "to improve patient care in the public interest." as exemplified by the "section 251 exemption." [68]

This section examines why these legal safeguards have not managed to prevent the failures in the management of medical data identified in the 2014 Partridge Review. It concludes that the current legislation does not address the potential for abuse and malfeasance.

NHS Constitution: patient rights: The NHS Constitution states the "right to privacy and confidentiality" and "the expectation that the NHS keeps confidential information safe and secure." [69] On top of this internal NHS Constitution, the Department of Health issued guidelines on privacy in the NHS Code of Conduct, placing greater emphasis on fairness than on the confidentiality of data processing itself [70]:

"The NHS is committed to the delivery of a first class confidential service. This means ensuring that all patient information is processed fairly, lawfully and as transparently as possible so that the public understand the reasons for processing personal information, give their consent for the disclosure and use of their information, gain trust in the way the NHS handles their information and understand their rights to access information held about them."

Patient Privacy and the Data Protection Act (1998): This Act, on the other hand, imposes explicit statutory conditions on data processing and aims to balance the legitimate need of organizations to collect data for defined purposes against the right of individuals to respect for the privacy of their personal details [71]. In the medical field, the Act states that organizations such as the NHS must ensure that any personal information it gathers be kept "secure." Furthermore, this Act lists the data protection responsibilities that apply to GPs in their capacity as "data controller." The key implication is that "data subjects" (i.e., patients) are entitled to seek compensation from the "data controller."

The Information Commissioner's Office Code of Practice is a statutory code approved by the Secretary of State that explains how the Data Protection Act 1998 applies to the sharing of personal data [72]. It lays out good-practice recommendations to guide organizations in collecting and sharing personal data in a way that is compliant with the law, transparent, and in line with the rights of the people whose data has been collected [72]. The Code of Practice does not have the force of law, and thus is not legally binding, but failure to follow its recommendations could lead to breaches of the Data Protection Act 1998 [72]. It is the Data Protection Act that sets out legally enforceable obligations [72].

Controversy over exemptions and the Health and Social Care Act (2012): This Act is key to understanding the controversial tensions within the care.data legal framework, as the Act conflicts with the NHS Constitution and the Data Protection Act. This Act empowers the HSCIC to be the sole extractor, storer, and dispenser of medical records. The HSCIC can share confidential data when the patient has given explicit consent and for two other reasons: the Police and Criminal Evidence Act 1984 and section 251 exemptions.

First, the Act acknowledges that there are circumstances in which the objections of patients (or "data subjects") may be overridden, for reasons ranging from criminal investigation to the prevention of pandemics, as stipulated in the Police and Criminal Evidence Act 1984.

Second, the Act permits the disclosure of data to public or private entities approved under the Regulation number 5 of the HSCIC, a controversial exemption often referred to as "Section 251." This section permits the Secretary of State for Health to set aside the common law duty of confidentiality in order to share confidential data without the consent of patients to actors whose purpose is "to improve patient care in the public interest." Such a purpose can be interpreted in a variety of ways. Applications from public and private entities to be granted access are reviewed by the Confidentiality Advisory Group (CAG), which monitors the purposes for which these records are needed. The parties must sign a data sharing agreement in order to obtain patient information with key identifiers such as name, address, NHS number and postcode removed.

As noted above, the passage of this Act means that GPs are pulled in two contradicting directions. HSCIC can command data from GPs under the Health and Social Care Act, but GPs also have obligations to patients to protect their data under the Data Protection Act [73].

R v. Department of Health: a contentious case law: The case law adds another complicating dimension to the requirements of confidentiality and anonymity. In 2001, the Court of Appeal held in *R v Department of Health, ex parte Source Informatics Ltd* that the disclosure of medical data to private parties does not breach confidentiality if the data is anonymous. Under this premise, information can be sold without the consent of patients. Doctors and pharmacists passing information about drug prescriptions to private companies were not considered guilty of breaking the confidence of their customers or patients. This case assumes that health data can in fact be anonymized and established the principle that data ceases to be personal and confidential once it has been made anonymous [74, 75].

EU and supranational legislation: Privacy is also a requirement of European human rights law. The protection of medical data falls under the scope of Article 8 of the European Convention on Human Rights (ECHR), and, as such, under the scope of the Human Rights Act 1998.

Article 8 ECHR protects the right to "private life," which entails, according to the case law, the protection of medical data. In *Z v Finland* (1997), the Court ruled that it was a duty of Member States to take affirmative steps to ensure high levels of medical confidentiality. As such, the UK is legally bound to develop a robust and trusted ethical and legal framework before it proceeds with the launch of care.data.

On case law**.** *I v Finland* is key to understanding ECHR's jurisprudence on medical data disclosure. The case concerned a female nurse, diagnosed as HIV positive, whose medical history had been consulted by her hospital colleagues without her consent. The applicant claimed that the accessibility of her medical data led to her dismissal on unfair grounds [76]. The ruling in this case placed a duty on public administrations to address their deficiencies in record keeping and to promote what is known as the "doctrine of positive obligations in relation to the protection of personal data." [77]

Additionally, the European Commission, Council, and Parliament are now in the process of writing a new General Data Protection Regulation (GDPR) in order to update the current EU 1995 Data Protection Directive 95/46/EC and uniformly strengthen digital privacy laws across the EU. In its current form, the Regulation draft could significantly challenge the validity of the care.data system [78].

Accountability and Regulation

The care.data program reveals NHS England's top-down culture, ratifying decision-making according to its own desired outcomes. It also exhibits a dysfunctional chronology: care.data was initially poised to be launched under the radar without democratic consultation or diverse viewpoints, then was subjected to multiple bodies of regulation in order to stay afloat, then came under increasingly greater scrutiny due to distrust. In an interview, Sam Smith of patient advocacy organization medConfidential noted that NHS England has deflected responsibility for the program, bearing the trademarks of unsuccessful policy: "If you ask various public bodies who is responsible for care.data, everyone will say NHS England, apart from NHS England, who will direct it on to someone else" [84]. To varying degrees, regulatory bodies have rallied around the fundamental premise that the public should be better consulted on care.data.

Care.data inquiry (All Party Parliamentary Group): The Health Select Committee launched an official inquiry through a series of evidence reviews to investigate the potential breaches of patient privacy at care.data. In November 2014 the All Party Parliamentary Group (APPG) for Patient and Public Involvement in Health and Social Care published the care.data inquiry, criticizing a "lack of clarity and publicity [79]." It wanted to investigate the communication of the care.data program with the public, the question and process of opting in or out, the impact of research sharing of data for patient care, who could gain access to medical care, and why.

The APPG consulted healthcare charities, royal colleges, the research community, and NHS England, organizations with "strong support for medical data sharing in theory" [79]. The inquiry established that:

- The public were "broadly supportive" of using health data for research that benefits the general public.
- Most of the public were in favor of an opt-out instead of an opt-in system to create datasets that were representative of the population and large enough to be reliable.
- There was unanimous agreement that the program hadn't been communicated properly to the public, and consultation was vitally needed.
- Legal accountability and penalties for those who breach patient data laws needed clarity.

Care.data advisory group: In response to the communications campaign backlash, NHS England established an independent panel composed of citizen-centric groups in March 2014. Its purpose was to address concerns with the care.data project and represent the interests of patients in the process of the care.data launch. It was led by Ciaran Devane, Chief Executive of Macmillan Cancer Support and NHS England non-executive director. Members included academics, research groups, regulators, health charities and NHS bodies. The panel began its work with a series of open meetings.

IIGOP report and Fiona Caldicott's National Data Guardian role: The Independent Information Governance Oversight Panel (IIGOP) is an NHS watchdog chaired by Dame Fiona Caldicott. Dame Caldicott is also the National Data Guardian, and "Caldicott Guardians" are senior figures throughout the health and social care systems who monitor decision-making around shared data.

An IIGOP report, **"**Information: to share or not to share," was commissioned by the Secretary of State in 2013 around sharing data and was finally released in January 2015. It raised multiple questions around care.data that had to be answered before care.data could be implemented. It also reviewed the progress of a Report on the Review of Information Governance by Fiona Caldicott, released in 2013.

Caldicott called for collective accountability for information governance and privacy in 2013: "Everyone working in the health and social care system should see information governance as part of their responsibility" [80], and reviewed the progress as a failure of this commitment. She also called attention to the fact that the Health and Social Care Act of 2012 led to "the loss of centers of expertise in information governance that had existed in Strategic Health Authorities and Primary Care Trusts. The emergence of new organizational structures at a time of financial stringency appears to have made it difficult

to employ sufficiently expert information governance staff." [80] A "fundamental change to professional and organizational culture" was required [80].

In an interview, Caldicott explained that "there needs to be cultural change rather than a legal or regulatory one." Under current scrutiny, she advocates for an approach of pioneering leadership in information governance, observing that "the difficulty is leadership in primary care, and is most varied in social care," recommending that "clinicians and social workers should have good induction training to link up social care to systems in health" [85].

National Information Board: The National Information Board was set up in December 2014, mandated by Health Secretary Jeremy Hunt. It brings together leaders and experts in health and social care as a body to discuss health information and governance, with a policy lens. The December meeting centered around a new report, "Personalised Health and Care 2020," which explored safe digital record keeping of patient data, giving the public greater access to and understanding of their data.

Discussion

What can We Learn, and Where will it End?

The general narrative of the care.data controversy is not UK-specific. Other European countries, such as the Netherlands and Austria, confronted similar media uproars when attempting to centralize medical data for cost-benefit purposes. Arguably, these controversies will become increasingly common against the backdrop of greater data collection and the growing imperative of privacy protection in human rights legislation.

The predominant public policy question that emerges from this review centers on how best to utilize technological advances and simultaneously strike a balance between the many competing interests around health and personal privacy. Our findings suggest that this balance may be able to be achieved if communication with the public is prioritized, the mechanisms to express consent are specific and easy to understand, control of data is decentralized or centralized only on a small scale, and regulations on purchasers of patient data are clearly outlined and subject to strong government oversight.

Multiple failures throughout this program provide lessons for large-scale IT project management. More specifically, care.data has gone wrong because of management and communication failures, misalignment of technical expectations and possibilities, and problems with the legal vacuum in which it was launched. This ultimately culminated in a lack of public understanding and consent required for a project of this magnitude and gravity.

We suggest that in its present form care.data should not be deployed because of inadequate protection of patient anonymity, a problematic opt-out system, unclear

criteria for accessing the data, and the risk it presents in eroding the trust between patients and GPs.

Whether care.data will achieve a re-balanced approach and be successfully implemented draws divergent opinions:

- **Ross Anderson, Professor of Security Engineering, University of Cambridge Computer Laboratory:** "The UK probably won't be as adventurous as to overthrow government policy for opt-in rather than opt-out, but Strasbourg might be." [83]

- **Sam Smith, Privacy International and MedConfidential:** "Until the scope of divergent buyers ... and the purposes of usage are explicitly outlined, then consent with the public and public acceptance cannot be gained, and the project will continue to be stalled." [84]

- **Fiona Caldicott, UK National Data Guardian:** "I don't think the public has been consulted sufficiently. If we knew the public was content with their data to be used for general health and social care purposes, that would be a huge step forward." [85]

Uncertainty characterizes the future of the care.data project. What remains undisputed is that public trust has been undermined. Any handling of the care.data project going forward must address this deficit and adopt a different approach to public engagement and project management. The integrity of population health, privacy rights, and the usage of data for public good demand nothing less.

References

1. BBC News. Everyone 'To Be Research Patient', Says David Cameron. December 5, 2011. http://www.bbc.co.uk/news/uk-16026827

2. UK Parliament. House of Commons Hansard. Column 141. February 25, 2014. http://www.publications.parliament.uk/pa/cm201314/cmhansrd/cm140225/debtext/140225-0001.htm

3. Flood G. Can British Docs Give Up Envelopes As Storage? Information Week. April 1, 2013. http://www.informationweek.com/healthcare/electronic-health-records/can-british-docs-give-up-envelopes-as-storage/d/d-id/1109334

4. Nuffield Council on Bioethics. The Collection, Linking and Use of Data in Biomedical Research and Health Care: Ethical Issues. 2015. http://nuffieldbioethics.org/wp-content/uploads/Biological_and_health_data_web.pdf

5. Cooper R. J. Information Technology, Ethics and Pharmacy Medicine Sales. In Robinson and Strain (Eds.), Ethics for Living and Working. Troubador Publishing Ltd. Leicester. 2008. http://www.troubador.co.uk/book_info.asp?bookid=669

6. Shetty & Partners. Care.data: What You Should Know. 2015. http://shettygp.nhs.uk/care-data-what-you-should-know

7. Chantler C, Clarke, T, Granger, R. Information Technology in the English National Health Service. The Journal of the American Medical Association. 296 (18), 2255-2258. 2006. http://jama.jamanetwork.com/article.aspx?articleid=203964

8. Health and Social Care Information Centre. Methodology For Creation of the HES Patient ID (HESID). 2014. http://www.hscic.gov.uk/media/1370/HES-Hospital-Episode-Statistics-Replacement-of-the-HES-patient-ID/pdf/HESID_Replacement_Nov09.pdf

9. Health and Social Care Information Centre. Secondary Uses Service (SUS). 2015. http://www.hscic.gov.uk/sus.

10. Nuffield Council on Bioethics. The Collection, Linking and Use of Data in Biomedical Research and Health Care: Ethical Issues. 2015. http://nuffieldbioethics.org/wp-content/uploads/Biological_and_health_data_web.pdf

11. Chantler C, Clarke, T, Granger, R. Information Technology in the English National Health Service. The Journal of the American Medical Association. 296 (18), 2255-2258. 2006. http://jama.jamanetwork.com/article.aspx?articleid=203964

12. Maughan A. Six reasons why the NHS National Programme for IT Failed. Computer Weekly. 2010. http://www.computerweekly.com/opinion/Six-reasons-why-the-NHS-National-Programme-for-IT-failed

13. King L. Update: NHS IT Programme Software 'Three Times Market Price.' Computer World UK. December 15 2011. http://www.computerworlduk.com/news/it-vendors/nhs-it-programme-software-three-times-market-price-3325079

14. Nuffield Council on Bioethics. The Collection, Linking and Use of Data in Biomedical Research and Health Care: Ethical Issues. 2015. http://nuffieldbioethics.org/wp-content/uploads/Biological_and_health_data_web.pdf

15. Department of Health. Dismantling the NHS National Programme for IT. Press Release. Department of Health. 2011. https://www.gov.uk/government/news/dismantling-the-nhs-national-programme-for-it

16. Nuffield Council on Bioethics. The Collection, Linking and Use of Data in Biomedical Research and Health Care: Ethical Issues. 2015. http://nuffieldbioethics.org/wp-content/uploads/Biological_and_health_data_web.pdf

17. Anderson R, Brown I, Dowty T, Inglesant P, Heath W, Sasse A . Database State: A Report Commissioned By the Joseph Rowntree Reform Trust Ltd. Joseph Rowntree Reform Trust. 2009. http://www.cl.cam.ac.uk/~rja14/Papers/database-state.pdf

18. Anderson R. Ross Anderson Website. Section: Security of Clinical Information Systems. 2015. http://www.cl.cam.ac.uk/~rja14

19. Nuffield Council on Bioethics. The Collection, Linking and Use of Data in Biomedical Research and Health Care: Ethical Issues. 2015. http://nuffieldbioethics.org/wp-content/uploads/Biological_and_health_data_web.pdf

20. NHS England Website. http://www.nhs.uk/nhsengland/thenhs/records/healthrecords/pages/overview.aspx

21. NHS England. Privacy Impact Assessment: Care.data. 2014. http://www.england.nhs.uk/wp-content/uploads/2014/01/pia-care-data.pdf

22. Nuffield Council on Bioethics. The Collection, Linking and Use of Data in Biomedical Research and Health Care: Ethical Issues. 2015. http://nuffieldbioethics.org/wp-content/uploads/Biological_and_health_data_web.pdf

23. UK Parliament. House of Commons. Committee of Public Accounts. Dr. Foster Intelligence: A joint venture between the Information Centre and Dr. Foster LLP. House of Commons. 2007. http://www.publications.parliament.uk/pa/cm200607/cmselect/cmpubacc/368/368.pdf 27

24. Heath N. How Big Data Can Save Lives by Diagnosing Healthcare Data. Tech Republic UK. 2014. http://www.techrepublic.com/article/how-big-data-can-save-lives

25. Health and Social Care Information Centre. Primary Care – Secondary Care Linkage. Presentation: Leeds – Stakeholder Forum. Presented by Trevor Anders. 2013. http://www.hscic.gov.uk/media/12354/stakeholder-forum-10-07-13-9linking-primary-and-secondary-care-data-for-commissioning-

purposes/pdf/Stakeholder_Forum_10-07-13-9_-_Linking_Primary_and_Secondary_Care_Data_for_Commissioning_Purposes.pdf

26. Nuffield Council on Bioethics. The Collection, Linking and Use of Data in Biomedical Research and Health Care: Ethical Issues. 2015. http://nuffieldbioethics.org/wp-content/uploads/Biological_and_health_data_web.pdf

27. Solon O. A Simple Guide to Care.data. Wired UK. 2014. http://www.wired.co.uk/news/archive/2014-02/07/a-simple-guide-to-care-data.

28. Health and Social Care Information Centre. General Practice Extraction Service (GPES): Customer Benefits Plan, Version 2.1. 2013. http://www.hscic.gov.uk/media/11704/Care-Data-IAG-Benefits-Plan---27-March-2013-NIC-178106-MLSXW/pdf/Care_Data_IAG_Benefits_Plan_-_27_March_2013_(NIC-178106-MLSXW).pdf.

29. Pulse Today. Q&A: NHS England's Care.data Programme. October 3, 2013. http://www.pulsetoday.co.uk/your-practice/practice-topics/it/qa-nhs-englands-caredata-programme/20004621.article#.VO4Jq2SsVsB.

30. Anderson R. 2014. Why Anonymity Fails. Open Data Institute. Lecture Conducted from Cambridge University. http://www.cl.cam.ac.uk/~rja14/Presentations/anonymity-fails-odi2014.pdf

31. Matthews-King A. Three in four GPs Believe Care.data Should Be 'Opt In.' Pulse Today. February 28, 2014. http://www.pulsetoday.co.uk/your-practice/practice-topics/it/three-in-four-gps-believe-caredata-should-be-opt-in/20005954.article#.VO4H52SsVsA

32. Solon O. A Simple Guide to Care.data. Wired UK. 2014. http://www.wired.co.uk/news/archive/2014-02/07/a-simple-guide-to-care-data.

33. Glick B. The Lesson From the NHS Care.data Row: You Can't Keep Privacy Issues Private Anymore. Computer Weekly. February 28, 2014. http://www.pulsetoday.co.uk/your-practice/practice-topics/it/three-in-four-gps-believe-caredata-should-be-opt-in/20005954.article#.VO4H52SsVsA

34. Ramesh R. NHS England Patient Data 'Uploaded to Google Servers,' Tory MP Says. The Guardian. March 3, 2014. http://www.theguardian.com/society/2014/mar/03/nhs-england-patient-data-google-servers.

35. Health and Social Care Information Center. Register of Approved Data Releases. 2014. http://www.hscic.gov.uk/media/13787/Register-of-approved-data-releases/pdf/Published_Version_Data_Releases_Register_v1.0.pdf

36. Ramesh R. NHS Patient Data to be Made Available for Sale to Drug and Insurance Firms. The Guardian. January 19, 2014. http://www.theguardian.com/society/2014/jan/19/nhs-patient-data-available-companies-buy.

37. Pulse Today. Q&A: NHS England's Care.data Programme. October 3, 2013. http://www.pulsetoday.co.uk/your-practice/practice-topics/it/qa-nhs-englands-caredata-programme/20004621.article#.VO4Jq2SsVsB

38. Nuffield Council on Bioethics. The Collection, Linking and Use of Data in Biomedical Research and Health Care: Ethical Issues. 2015. http://nuffieldbioethics.org/wp-content/uploads/Biological_and_health_data_web.pdf

39. Ipsos MORI. Privacy and Personal Data. 2014. https://www.ipsos-mori.com/Assets/Docs/Polls/jrrt-privacy-topline-nhs-2014.pdf

40. Nuffield Council on Bioethics. The Collection, Linking and Use of Data in Biomedical Research and Health Care: Ethical Issues. 2015. http://nuffieldbioethics.org/wp-content/uploads/Biological_and_health_data_web.pdf

41. Pulse Today. Q&A: NHS England's Care.data Programme. October 3, 2013. http://www.pulsetoday.co.uk/your-practice/practice-topics/it/qa-nhs-englands-caredata-programme/20004621.article#.VO4Jq2SsVsB

42. Matthews-King A. Three in Four GPs Believe Care.data Should Be 'Opt In.' Pulse Today. February 28, 2014. http://www.pulsetoday.co.uk/your-practice/practice-topics/it/three-in-four-gps-believe-caredata-should-be-opt-in/20005954.article#.VO4H52SsVsA

43. Vallance C. Adults 'Unaware of NHS Data Plans.' BBC News. February 14, 2014. http://www.bbc.co.uk/news/health-26187980

44. Goldacre B. Care Data is in Chaos. It Breaks My Heart. The Guardian. February 28, 2015. http://www.theguardian.com/commentisfree/2014/feb/28/care-data-is-in-chaos.

45. Pulse Today. Care.data Practice Pilots Will Not Start Until 2015. December 16, 2014. http://www.pulsetoday.co.uk/your-practice/practice-topics/it/caredata-practice-pilots-will-not-start-until-2015/20008752.article.

46. Swinford, S. NHS Legally Barred from Selling Patient Data for Commercial Use. 2014. http://www.telegraph.co.uk/news/health/10669295/NHS-legally-barred-from-selling-patient-data-for-commercial-use.html

47. Glick B. The Lesson From the NHS Care.data Row: You Can't Keep Privacy Issues Private Anymore. Computer Weekly. February 28, 2014. http://www.pulsetoday.co.uk/your-practice/practice-topics/it/three-in-four-gps-believe-caredata-should-be-opt-in/20005954.article#.VO4H52SsVsA

48. Ramesh R. January 19, 2014. NHS patient data to be made available for sale to drug and insurance firms. The Guardian. http://www.theguardian.com/society/2014/jan/19/nhs-patient-data-available-companies-buy.

49. Health and Social Care Information Center. Register of Approved Data Releases. 2014. http://www.hscic.gov.uk/media/13787/Register-of-approved-data-releases/pdf/Published_Version_Data_Releases_Register_v1.0.pdf

50. Matthews-King A. Care.data to be Piloted in GP Practices Before Full Rollout. Pulse Today. April 23, 2014. http://www.pulsetoday.co.uk/your-practice/practice-topics/it/caredata-to-be-piloted-in-gp-practices-before-full-rollout/20006498.article#.Va4dTUtsAdu.

51. Sachdeva, S. Care.data in "Last Chance Saloon." Digital Health. January 2015. http://www.digitalhealth.net/news/ehi/9844/care.data-in-/

52. Partridge Sir N. Review of Data Releases by the NHS Information Centre. Health and Social Care Information Centre. 2014. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/367788/Sir_Nick_Partridge_s_summary_of_the_review.pdf

53. NHS England News. CCGs to Help Develop Care.data Programme. Press release. 2014. http://www.england.nhs.uk/2014/10/07/ccgs-care-data-programme/

54. Health and Social Care Information Centre. What Types of Data Can be Released, for Which Purposes, to Which Organisations, and Under What Lawful Basis. 2015. http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/health-committee/handling-of-nhs-patient-data/written/17671.pdf

55. medConfidential. How To Opt Out. https://medconfidential.org/how-to-opt-out/

56. Pulse Today. HSCIC Promises Not to Count Care.data Opt Out at GP Practice Level. February 23, 2015. http://www.pulsetoday.co.uk/your-practice/practice-topics/it/nhs-england-promises-not-to-count-caredata-opt-outs-at-gp-practice-

level/20009267.article?utm_content=buffer27eb9&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer#.VO4Na2SsVsB

57. Jee C. Care.data: Main Milestones For Controversial Health Data Sharing Scheme. Computerworld UK. June 11, 2015. http://www.computerworlduk.com/galleries/data/caredata-main-milestones-controversial-health-data-sharing-scheme-3616561.

58. British Medical Association. Confidentiality and Health Records. A Report. 2014. http://bma.org.uk/practical-support-at-work/ethics/confidentiality-and-health-records/care-data

59. Ramesh R. NHS England Patient Data 'Uploaded To Google Servers,' Tory MP Says. The Guardian. 2014. http://www.theguardian.com/society/2014/mar/03/nhs-england-patient-data-google-servers

60. Pulse Today. Patient Records Handed Out To 56 Private Sector Organisations Data Controller Reveals. April 3, 2014. http://www.pulsetoday.co.uk/your-practice/practice-topics/it/patient-records-handed-out-to-56-private-sector-organisations-data-controller-reveals/20006347.article#.VO4OhGSsVsB.

61. Health and Social Care Information Center. Register of Approved Data Releases. 2014. http://www.hscic.gov.uk/media/13787/Register-of-approved-data-releases/pdf/Published_Version_Data_Releases_Register_v1.0.pdf

62. Ferreira A, Cruz-Correia R, Antunes L, Chadwick D. Access Control: How Can It Improve Patients' Healthcare? Medical and Care Compunetics Volume 4 in Series in Health Technology and Informatics 27. 2007. https://kar.kent.ac.uk/14578/1/Access.pdf

63. Burton G. Privacy Under The Knife: Can Care.data Be Trusted? Computing UK. 2014. http://www.computing.co.uk/ctg/feature/2326227/privacy-under-the-knife

64. Health and Social Care Information Center. The DAAG Approval Process. http://www.hscic.gov.uk/article/2194/The-DAAG-approval-process

65. Health and Social Care Information Centre. Data Release Review. PricewaterhouseCoopers. 2014. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/367791/HSCIC_Data_Release_Review_PwC_Final_Report.pdf.

66. Herring J. Medical Law and Ethics. Oxford, U.K.: Oxford University Press. 2014. http://ukcatalogue.oup.com/product/9780198702269.do

67. Caldicott F. The Information Governance Review. Department of Health. 2013. https://www.gov.uk/government/publications/caldicott-information-governance-review-department-of-health-response

68. Nuffield Council on Bioethics. The Collection, Linking and Use of Data in Biomedical Research and Health Care: Ethical Issues. 2015. http://nuffieldbioethics.org/wp-content/uploads/Biological_and_health_data_web.pdf

69. Department of Health. The Handbook to the NHS Code of Practice. 2013. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/170649/Handbook_to_the_NHS_Constitution.pdf

70. Department of Health. The NHS Code of Practice. 2003. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/200146/Confidentiality_-_NHS_Code_of_Practice.pdf.

71. The General Practitioners Committee. The Data Protection Act 1998: An Updated Code of Practice for GPs. BMA. 2000. https://www.igt.hscic.gov.uk/KnowledgeBase/KB%5CGeneral%20Practitioners%20Committee%5CGPC%20Guidance%20on%20the%20Data%20Protection%20Act%201998.pdf

72. Information Commissioner's Office (ICO). Data Sharing Code of Practice. 2014. https://ico.org.uk/media/fororganisations/documents/1068/data_sharing_code_of_practice.pdf

73. Nuffield Council on Bioethics. The Collection, Linking and Use of Data in Biomedical Research and Health Care: Ethical Issues. 2015. http://nuffieldbioethics.org/wp-content/uploads/Biological_and_health_data_web.pdf

74. Herring J. Medical Law and Ethics. Oxford, U.K.: Oxford University Press. 2014. http://ukcatalogue.oup.com/product/9780198702269.do

75. Commentary. Breach of Confidence: Anonymised Information. Medical Law Review (8)1. 2000. http://www.ncbi.nlm.nih.gov/pubmed/11787501

76. Fink U. Protection of Privacy In The EU, Individual Rights and Legal Instruments. In Witzelb N, Lindsay D, Paterson M, Rodrick S. (Eds.), Emerging Challenges in Privacy Law: Comparative Perspectives (Cambridge Intellectual Property and Information Law). Cambridge: Cambridge University Press. 2014. http://www.cambridge.org/sv/academic/subjects/law/intellectual-property/emerging-challenges-privacy-law-comparative-perspectives

77. Gonzalez Fuster G. The Emergence of Personal Data Protection as a Fundamental Right of the EU. Springer International Publishing. 2014. http://www.springer.com/us/book/9783319050225

78. Saran C. EU Data Protection Reform Threatens NHS Record-Sharing Plans. ComputerWeekly.com. 2014. http://www.computerweekly.com/news/2240230763/EU-data-protection-reform-threatens-NHS-record-sharing-plans

79. The All Party Parliamentary Group for Patient and Public Involvement in Health and Social Care. Care.data inquiry. 2014. http://patients-association.com/wp-content/uploads/2014/06/APPG-Report-on-Care-data.pdf

80. IIGOP. Information: To Share Or Not To Share – The Independent Information Governance Oversight Panel's Report To The Secretary Of State For Health. Department Of Health. 2015. https://www.gov.uk/government/publications/iigop-annual-report-2014

81. Interview with Paul Cundy. Kancir J. February 18, 2015.

82. Interview with Deborah Peel. Presser L. February 20, 2015.

83. Interview with Ross Anderson. Rowbottom H., Hruskova M., Presser L. February 18, 2015.

84. Interview with Sam Smith. Rowbottom H. February 17, 2015.

85. Interview with Dame Fiona Caldicott. Rowbottom H. February 23, 2015.

Authors

Lizzie Presser is a Gates Cambridge scholar who completed her MPhil in Public Policy at the University of Cambridge.

Maia Hruskova completed her MPhil in Public Policy at the University of Cambridge and focuses on the intersection between law and politics.

Helen Rowbottom completed an MPhil in Public Policy at the University of Cambridge in 2015, having been granted a scholarship from Queens' College, Cambridge.

Jesse Kancir is an MD, and completed an MPhil in Public Policy as a Chevening Scholar.

Editor: Ross Anderson

Citation

Presser L, Hruskova M, Rowbottom H, Kancir J. Care.data and access to UK health records: patient privacy and public trust. *Technology Science*. 2015081103. August 11, 2015. http://techscience.org/a/2015081103

Data

See References for sources