For Health Select Committee Evidence session, 25/2/14
from Phil Booth for medConfidential - coordinator@medconfidential.org

Summary

medConfidential is an independent, non-partisan, not-for-profit organisation - a Company Limited by Guarantee with charitable objects - which campaigns to preserve and strengthen confidentiality and consent in health and social care. medConfidential's goal is for every data flow into, within and out of the NHS and social care system to be consensual, safe and transparent in ways that patients and service users are aware of and can understand.

We have divided our written submission to the Committee into four parts:

- Summary and questions
- Specific issues
- Timeline of policy shifts
- Attachments

We recommend to the Committee the recent ESRC/ADLS announcement on the funding of SCIF-style[1] "Sensitive Data Secure Rooms"[2] for academic access to highly sensitive data from DWP, DfE and the NHS for the purposes of *bona fide* academic research. We believe that such an approach, properly implemented, can generate the benefits of research data use with understandable and manageable risks to privacy. See 'Safe' section below for an outline suggestion on this. We further note that protections such as those in the Statistics and Registration Service Act 2007, or any equivalents, do not apply to care.data.

We agree with Ben Goldacre that "NHS England have been incompetent & arrogant over #caredata. It will save lives, if we can persuade them to unfuck it".[3] This is what medConfidential has now been working on for over a year. The issue with care.data is not merely one of inadequate and misleading communication, and a further delay is not enough.[4] If lives are to be saved, the entire programme needs to be fundamentally reengineered from the ground up - with informed public debate and contributions from all interested parties, not just NHS England's existing partners.[5]

All sides will claim to be interested in patient safety, and cases made for these claims should be subject to public debate and scrutiny. The last "public safety" issue that this Committee looked at was the PIP breast implants failure in 2012, and this Committee's inquiry

[1] http://en.wikipedia.org/wiki/Sensitive_Compartmented_Information_Facility
[2] http://www.adls.ac.uk/wp-content/uploads/ESRC-sensitive-data-secure-rooms.pdf
[3] https://twitter.com/bengoldacre/status/437308062484164608
[4] https://twitter.com/tkelsey1/status/437012983894773760
[5] Tim Kelsey on BBC Radio 4's Today programme, Wednesday 19th February 2014

recommended monitoring of implant failures. We note that the current version of the care.data GP extract would provide no information for such monitoring or early monitoring. This data is collected within GP practice systems, but was not deemed important enough for inclusion by NHS England when the care.data specification was designed. Why not?

Further questions

1) Patient opt out: As we cover in more detail in the timeline below, the opt out ('dissent') codes for care.data are only now being corrected to operate in the way that they should have from the start. We received a letter from the HSCIC's Director of Clinical and Public Assurance confirming this on the day the latest 6 month delay was announced. When will this be publicly announced? And why was HSCIC told to commission the dissent codes in such a way as to flow any data whatsoever from the GP records of patients who had opted out?

2) Data leaving the UK: The fact that data can be passed to organisations outside of UK's jurisdiction tends to undermine the claim - and stated goal - of the care.data scheme that it will drive economic growth in the UK. Quite aside from the obvious concerns this may raise for many patients, on what basis will NHS England or HSCIC decide to allow patient data to be shared outside of the EEA?[6]

3) Lack of independent oversight and transparency: As we cover in the section on transparency below, and despite what the public and GPs have been told, the body that approves access to sensitive patient-level data (DAAG) lacks independent scrutiny, has potential conflicts of interest and has on a number of occasions made unminuted, out-of-committee decisions on the provision of sensitive data. HSCIC as a whole provides inadequate and incomplete information about the organisations and companies that have been provided data.

- Why was no suitably independent oversight body - on the model of something like the Confidentiality Advisory Group at the Health Research Authority - put in place for all disclosures of patient-level data?
- When will a complete Register of all data disclosures, with details of the organisations to which data was passed or sold and the stated use of the data be published?
- When will the independent and internal audits of the security and usage of HES and HES/SUS data be published? If NHS England claims there has been no breach or unauthorised use by the Information Center or any of its customers in 25 years, then - in the spirit of transparency, if nothing else - the public should be shown the evidence.

4) Misleading the public: It has become clear that NHS England has provided misleading

[6] http://www.healthcareitnews.com/news/us-uk-sign-bilateral-health-it-accord

information to the public - and possibly Ministers - on matters such as the distribution of its junk mail leaflet to all households[7], the operation of the patient opt out and the ability of patients to to change their minds at any time[8], and the sale of data to insurers for insurance purposes.[9] We cover most of these in more detail later in our evidence, but if NHS England wishes to regain the public trust, when will it publicly apologise for misleading the public on these matters?

5) Limited engagement: Thus far a large part of NHS England's engagement appears to have been with partners or stakeholders with either an interest in gaining access to patient data, or who handle it already. Such stakeholders may not have provided sufficiently robust challenge to the programme as it was developed. The Director of Patients and Information said last week that he will engage with partners going forward[10]. Will that engagement include all stakeholders, including patients themselves[11] and organisations who are not already partners?

There are many questions that needs answers, in order to satisfy Ben Goldacre's goal, "The NHS plan to share our medical data can save lives: but first they have to stop cocking it up." [12]

[7] https://www.whatdotheyknow.com/request/royal_mail_contract_for_caredata#incoming-484935

[8] http://www.leighday.co.uk/News/2014/February-2014/Legal-action-taken-day-before-NHS-patient-data-sha

[9] http://www.telegraph.co.uk/health/healthnews/10656893/Hospital-records-of-all-NHS-patients-sold-to-insurers.html

[10] Tim Kelsey on BBC Radio 4's Today programme, Wednesday 19th February 2014

[11] https://www.whatdotheyknow.com/request/patient_involvement_in_the_co_de#outgoing-335792

[12] https://twitter.com/bengoldacre/status/436950557409153024

Specific issues

medConfidential proposes three tests for data sharing: "consensual, safe and transparent". These are not rigid absolutes but should be taken together as a whole, in balance. Notifiable diseases do not require consent, for example, but those reports are both safe and transparent.

Consensual

It is understood that it it is not always possible to seek consent for every use of patients' data, and that the legal basis for setting aside the common law duty of confidentiality resides in Regulation 5 of The Health Service (Control of Patient Information) Regulations 2002, and Section 251 of the NHS Act 2006.

Our concern with the use of identifiable patient data lies in Regulation 5 / Section 251 support granted for indeterminate periods of time, applying to the majority of all primary and secondary care health records[13] for non-research purposes, especially when such extraordinary measures are granted ostensibly "to enable business critical activities to continue" but remain unused. A case in point would be the s251 support for data to be transferred from HSCIC to 'Accredited Safe Havens' in commissioning bodies, under which no data flowed from May to October 2013, but which was extended for a further 12 months last October with an understanding that it was likely to be extended again.[14]

This is particularly worrying as in public communications about care.data, the use of identifiable patient data has been presented as something done in exceptional circumstances, such as "in case of a public health emergency"[15] rather than as a matter of routine in commissioning or invoice reconciliation. We note that the Caldicott Information Governance Review report (Caldicott2) did not support the proposition that commissioning required identifiable patient data, stating "If identifiable data is to be used, a clear justification and a legal basis for doing so must be established and made known to patients."[16]

Properly informed consent, freely given by those with the capacity to do so, tends to build trust. Using the law to override or route around consent, or presuming consent for purposes other than someone's direct medical care not only offends common decency but violates people's fundamental human right to a private family life. And it is corrosive of trust.

---

[13] p31 http://www.hra.nhs.uk/documents/2014/01/cag-meeting-minutes-28-november-2013-3.pdf
[14] p3 http://www.hra.nhs.uk/documents/2014/01/cag-meeting-minutes-4-october-2013-2.pdf
[15] http://www.nhs.uk/NHSEngland/thenhs/records/healthrecords/Pages/care-data.aspx
[16] Caldicott review: information governance in the health and care system https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/192572/2900774_InfoGovernance_accv2.pdf

Treating every man, woman and child in England as a "research patient" without informed consent is repugnant to many people, contrary to international standards of research conduct [17] and is liable - via publishability issues, if nothing else - to blow up in the face of universities, interfere with development of evidence-based medical and social care, and reduce the financial value to the pharmaceutical and health products businesses.

medConfidential believes that if as much effort were expended on developing proper consent mechanisms and processes as is spent on other aspects of system design, the result would be enhanced trust. Running an opt in scheme initially, for example, would allow the public to see actual benefits rather than simply be told about speculative gains. Were an opt in 'plateau' to be reached, the government would be better able to determine the necessity and consequences of any measures required to achieve fuller participation, e.g. through an opt out approach.

Consent is, of course, not simply a matter of opt in or opt out. The ability for people to view their own information, to find out who has accessed it, to correct errors and have their data deleted if they withdraw consent are just as important - arguably more important - than a one-off indication of consent or dissent.

Safe

In a health context, the primary consideration must be for patients' well being. Confidentiality is fundamental in this regard. For if patients cannot trust that what they say to their doctor will be kept in confidence, then some may withhold information or simply not visit the doctor at all - putting not only their own health at risk, but in some instances the public health as well. NHS England recognises this in its recently-published care.data Privacy Impact Assessment:

The extraction of personal confidential data from providers without consent carries the risk that patients may lose trust in the confidential nature of the health service.

medConfidential contends that this is one of the most significant risks of the entire scheme, and that trust has already been lost due to the inappropriate design, and mishandling and miscommunication of care.data to date.

It is possible to handle data safely. Data minimisation and data security procedures, properly implemented, can give *bona fide* researchers and others access to data required for research and other rigorously-defined purposes. We note the recent ESRC announcement of "Sensitive Data Secure Rooms"[18] for academic research, and believe that, if a

[17] World Medical Association Declaration of Helsinki
http://www.wma.net/en/30publications/10policies/b3/
[18] http://www.adls.ac.uk/wp-content/uploads/ESRC-sensitive-data-secure-rooms.pdf

population-scale database of patient-level medical histories is to be created over time, then it must be protected by the best security our country knows how to deploy.

This is not simply a matter of processing patient data to remove some of the most obvious identifiers before passing or selling it on to others. What is required is a complete process and set of procedures commensurate to the immense value of this 'national treasure'.

There should, for example, only ever be one primary copy of the database. Those wanting access should not merely have to provide a plausible use or purpose, but should rather have to submit the specific query or queries they want to run on the database to an independent body of experts which can assess their likely outcome. If approved, a query may be run but before any results leave the secure facility another independent body of experts must check the pseudonymisation and other measures applied to ensure that particular dataset is as safe as possible, e.g. in case of data breach - which would, in effect, put the data on the black market for ever..

Such an approach would permit legitimate use of population-scale patient-level data without handing it to third parties to process themselves, thereby massively reducing the risk of harm in case of breach, misuse or abuse. The approach would also facilitate a genuine opt out for patients at any point, as opposed to the current care.data approach where once a patient's data has been uploaded it will never be deleted.

Pseudonymisation

Replacing NHS numbers, postcodes and dates of birth with pseudonyms is necessary and good practice, but it is not sufficient. In public communications thus far, NHS England has placed too much emphasis on this technical approach which is actually a bit of a red herring. Patient-level episodic health data, such as would be extracted from people's GP-held medical records under the care.data scheme, is inherently identifying. Removing or obscuring some of the most obvious identifiers will not prevent individuals being identified within the data.

For example, those in the public domain often get minor events reported, and even the most private individuals can find themselves in the newspaper due to an accident. Standard journalistic practice means that accidents reported in the local press will include the date of the event, a person's name and age, along with the area of town (or in some cases even the road) where the victim lives. Such reports usually provide enough information for an informed guess at likely diagnoses, which can be matched with a particular incident.

How many women of a particular age reported to a particular hospital with an elbow injury, the day that Nick Clegg's wife broke her elbow in 2010, just before the general election?[19]

[19] https://www.google.com/search?q=nick+clegg+wife+election+elbow+broken

The head of the Harvard Data Privacy Lab, Dr Latanya Sweeney has shown that almost everyone whose health included an event that was newsworthy was identifiable in de-identified data, using just the information available from media reports of that event. When contacted by the project, patients were horrified that the hospital knew of incidents in their past, and had then shared that data[20].

care.data - or more strictly, Care Episode Statistics (CES), the product of linked Hospital Episode Statistics (HES), the GP extract and other datasets - would not simply provide details of the diagnosis a patient has received in one incident, but other diagnoses and every prescription known for that same patient, including dates.

So another approach that might be used with episodic data might simply involve filtering across a number of dates; given the number of patients who visited a clinic on one date, one could search within that group for those who visited the clinic on another date, and so on. It is obvious that one will quite rapidly arrive at an individual record within the data, at which point the rest of that person's medical history can be read off.

Claiming that this will never happen, when the intention is to pass on or sell data to an expanded range of public and private sector organisations and companies is not credible.

Transparent

The culture, seemingly prevalent at NHS England, that allows institutional priorities to override patient choice and medical ethics without patient awareness, is the antithesis of transparency.

The rest of the public sector, following a decision by the Cabinet Office, are becoming more transparent about reporting some categories of issue to the Information Commissioner. Yet that requirement does not appear to apply to the categories of data about which we are most concerned.

We await a response to our Freedom of Information request to NHS England for the independent and internal audits of security and data usage for the existing HES and HES/Secondary Usage Service (SUS) systems. We note that there seems to be no requirement to report privacy incidents involving HES data[21] and are sceptical of claims that no privacy breach has occurred, especially as we work with someone who suffered harm and distress as a result of being incorrectly coded as an alcoholic, and having that passed around via the SUS - not to mention the prevalence of unauthorised access by authorised users in similar systems.

[20] http://www.youtube.com/watch?v=N4HTHyduQzE
[21] https://www.whatdotheyknow.com/request/independent_audits_of_hessus_and

Without full disclosure of the independent and internal audits done of both HSCIC systems, and every 'customer' to which HSCIC has provided data, the public can have little confidence in mere assertions from officials who have misled them in other ways. At the time of writing, we have received none of the information we asked for in our FOI request.

The transparency of every instance of sharing patient data - in whatever form - must be proactive and complete. HSCIC should not, for example, be making out-of-committee decisions to share data with Government Departments.[22] All accesses by or provision of data to third parties[23] should be fully reported to the public. Experience with the Department for Education's National Pupil Database shows that when usage of other sensitive datasets become transparent,[24] there are fewer concerns around use, and those concerns are grounded in particular uses, not abstract possibilities.

The Data Access Advisory Group (DAAG) at HSCIC and other processes around the release of data to third parties are quite clearly unfit for purpose. With only four of DAAG's members publicly known, of which two are from HSCIC and one from the Department of Health[25], the GPES Independent Advisory Group which assesses applications to extract data from GP practice systems has expressed concerns that DAAG "would benefit from including more external members", that it "did not reflect an appropriately broad range of perspectives", that it suffered from a lack of "independent scrutiny to determine whether data disclosure would be in the public interest" and that there could be a perceived "conflict of interest for HSCIC staff to determine whether or not a customer should receive data without any external input".[26]

Beyond DAAG itself, the GPES Independent Advisory Group rightly pointed out that "applications for data that were not considered sensitive would normally be signed off by the relevant HSCIC information asset owner rather than being considered by an independent group, and that as the general practice extract for care.data would not include Read codes categorised as sensitive it could follow this process".

medConfidential submits that oversight and transparency at HSCIC is broken, has been for some time and must be addressed as a matter of utmost urgency before any more data - and not just that gathered under the care.data scheme - is passed on or sold to third parties.

---

22 http://www.theguardian.com/politics/2014/feb/10/mark-davies-chairman-health-social-care-information-centre-to-depart

23 http://www.telegraph.co.uk/health/healthnews/10656893/Hospital-records-of-all-NHS-patients-sold-to-insurers.html

24 https://www.whatdotheyknow.com/request/requests_for_access_to_national#incoming-340035

25 http://www.hscic.gov.uk/daag

26 http://www.hscic.gov.uk/media/12911/GPES-IAG-Minutes-for-12-September-2013/pdf/GPES_IAG_Minutes_12.09.13.pdf

Timeline: the many policy shifts of NHS England

As originally envisaged by NHS England, at the point when the scheme first came to public attention in early 2013, "Ministers insisted there would be no opportunity to opt out".[27] We presume this position was based on the interaction between section 254 of the Health and Social Care Act 2012 which provides powers to *direct* HSCIC to establish information systems and/or section 255 regarding *mandatory requests* and section 259 which empowers HSCIC, if so directed, to *require* any person to provide it with information.

After an initial meeting between Privacy International and Tim Kelsey at which concerns were raised and no assurances were received, Privacy International and Big Brother Watch (two of medConfidential's founder organisations) and the newly formed medConfidential engaged with the Department of Health. It was our understanding at that point that NHS England intended some form of 'tribunal' process for patients who objected to the use of their medical information for purposes other than their direct care.

We were somewhat reassured that, at least in part as a result of our engagement, at the launch of the Caldicott2 report in April 2013 the Secretary of State for Health stated,[28] "The guidance that we will be giving to GPs is that if people ask for data not to be shared, then it won't be... If people ask for their information not to go beyond the GP's surgery, GPs will respect that" and further, "We will respect people who have already said they have opted out of any data sharing".

This clear commitment was almost immediately watered down by officials at NHS England. As it stands, some 640,000+ patients[29] who have opted out of other forms of data sharing such as the Summary Care Record must now take action to opt out once again. This is the sort of behaviour that prompts public and Parliamentary condemnation when it is used by Facebook[30] or Google[31] to boost the data they can use for other ('secondary') purposes.

By September 2013, after further questions from medConfidential and with the involvement of the Information Commissioner's Office - which, at the point we alerted them, had not held a single formal meeting with NHS England on care.data[32] - NHS England had dropped the tribunal approach and was offering what appeared to be the opt out promised by the Secretary

---

27 http://www.dailymail.co.uk/news/article-2315003/U-turn-NHS-database-opt-Victory-privacy-campaign-hunt-backs-down.html

28 https://www.youtube.com/watch?v=Udpaajqg3nE

29 http://nhscfhscr.createsend1.com/t/ViewEmail/r/DC91206E959D97B32540EF23F30FEDED - "Of the 45,997,228 people contacted, just 1.4% opted out" = 643,961 for SCR alone, not including other opt outs

30 http://news.bbc.co.uk/1/hi/8405334.stm

31 http://news.bbc.co.uk/1/hi/8603155.stm

32 e-mail from Dawn Monaghan, Group Manager, Public Services at the ICO, 10/4/13

of State.

However, its approach to informing patients of the scheme and of their right to opt out up to that point had been completely inadequate, amounting to little more than a poster and some leaflets put in GP practice receptions over the summer of 2013[33]. The ICO decided that this would not constitute fair processing under the Data Protection Act, and - despite having ruled out a national publicity campaign just the month before[34] - NHS England was forced to delay the first care.data uploads until March 2014 and come up with a more appropriate public communications programme.

The Committee will by now be aware of the inadequacies of NHS England's second communications programme, the heart of which was a junk mail leaflet sent to millions of households across England. But not, as has been claimed[35], to all households. We further believe that the leaflet was misleading and on 17th February 2014 medConfidential instructed Leigh Day Solicitors to send a letter before action questioning the legal accuracy of NHS England's public information campaign[36].

medConfidential has stated from the outset that the appropriate form of communication to patients in this context would be a letter directly addressed to them in person, as was done for the roll-out of the Summary Care Record. We would not consider such a letter sufficient by itself, and believe that the process should be opt in rather than opt out. But if the process is to be an opt out, then of course an opt out form must be included with any communication.

It is therefore odd to hear the Secretary of State for Health reported as saying, "The reason we're having [a heated public debate] is because [Kelsey] decided to send a leaflet to every household to tell them about what was happening and the result of that is we will earn the trust of the public because we're being open about it and giving them a chance to opt-out"[37] when this was hardly a decision by choice - Mr Kelsey had do something after NHS England's initial communication was deemed inadequate, and possibly unlawful.

It is equally strange to see Mr Kelsey himself tweeting last week, "I absolutely pushed for opt out - you know me"[38] It seems the Director for Patients and Information at NHS England may

---

[33] See FAQ 6 in the information sent to GP practices at this point: https://web.archive.org/web/20131102105136/http://www.england.nhs.uk/wp-content/uploads/2013/08/cd-faqs.pdf

[34] http://www.pulsetoday.co.uk/your-practice/practice-topics/it/nhs-managers-rule-out-publicity-campaign-for-controversial-data-extract-programme/20003971.article

[35] Under-Secretary of State for Health to Parliament: http://www.theyworkforyou.com/wrans/?id=2014-02-03a.185177.h

[36] http://www.leighday.co.uk/News/2014/February-2014/Legal-action-taken-day-before-NHS-patient-data-sha

[37] http://www.ehi.co.uk/news/EHI/9205/nhs-will-be-dependent-on-ehrs----hunt

[38] https://twitter.com/tkelsey1/status/436982189855879168

be trying to rewrite history.

Most concerning was the discovery that, contrary to what the Secretary of State for Health had promised patients, repeated public statements by NHS England officials and the most reasonable interpretation of what was said in the junk mail leaflet, significant amounts of data would be extracted from the GP records of those patients who had opted out.

This was confirmed by NHS England's own Privacy Impact Assessment, which states:

Where patients have objected to the flow of their personal confidential data from the general practice record, the HSCIC will receive clinical data without any identifiers attached (i.e. anonymised data).

Setting aside the fact that de-identified data is not 'anonymised', except maybe in NHS technical parlance, this is quite clearly not what any reasonable person would expect by an opt out.

medConfidential therefore wrote to the Secretary of State on 12th February 2014, with a set of questions about the current policy shifts. At the time of writing, we have not yet received a an answer to that set of questions, though on Tuesday 18th February we received confirmation from the outgoing Director of Clinical and Public Assurance at HSCIC that the operation of the opt outs are in the process of being changed to what they should have been in the first place.

On that same day, Tuesday 18th, NHS England announced a second 6 month delay in data extraction - though it left open the possibility of extraction from some 'pilot' practices. And on that day as well, but without announcement, HSCIC updated the specification of the GP extract to correct errors found in a detailed audit after medConfidential had raised specific queries. We await an update on a third possible code error about which we notified HSCIC immediately on discovering that it had not been addressed.

Phil Booth
Coordinator, medConfidential
24 Feb 2014

Attachments

Enc, letter from Dr Mark Davies, dated 18 February 2014.

We would be happy to provide copies of our correspondence with the Secretary of State for Health, if the Committee requests.

hscic Health & Social Care Information Centre

1 Trevelyan Square
Boar Lane
Leeds
LS1 6AE

enquiries@hscic.gov.uk
www.hscic.gov.uk

18 February 2014

By E-mail

Phil Booth and Terri Dowty
medConfidential

Dear Phil Booth and Terri Dowty

Thank you for your letter.

In order to enable the HSCIC to apply the most recent objection codes regarding the release of a patient's identifiable data, the HSCIC proposes to extract data about these objection codes and the withdrawal of them. The General Practice Extraction Service (GPES) will return aggregate counts of the numbers of each type of objection recorded. Where a patient objects to information containing data that identifies them from leaving their GP practice (type 1 objection), only the aggregate counts along with the GP practice identifier will be returned by GPES. No other additional data will be extracted.

Where a patient objects to information containing data that identifies them from leaving the HSCIC (type 2 objection) the HSCIC proposes to extract the fact that a type 2 objection has been recorded, the date of that objection and the patient's NHS number. This extract will also include the GP practice identifier. The NHS number will be used internally within the HSCIC to match data held for that patient so that data can be de-identified before release.

Where a patient raises both a type 1 and type 2 objection it will be necessary to take the patient's NHS number in order to enable their wishes in respect of a type 2 objection to be implemented.

This proposal will be considered by the GPES Independent Advisory Group (IAG) in February for their confirmation.

Yours sincerely

Dr Mark Davies
Director of Clinical and Public Assurance