What does medConfidential mean by “consensual, safe and transparent”?

medConfidential proposes three tests for data sharing; that it should be "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 such collections and reports are both safe and transparent.

Consensual

It is understood that it is not always possible to seek consent for every use of patients’ identifiable 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 the use of Regulation 5 / Section 251 support granted for indeterminate periods of time, applying to the majority of all primary and secondary care health records[1] 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.[2]

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”[3] 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.”[4]

Well-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.

Treating every man, woman and child in England as a "research patient" without their knowledge and consent is repugnant to many people, contrary to international standards of

[1] p31 http://www.hra.nhs.uk/documents/2014/01/cag-meeting-minutes-28-november-2013-3.pdf
[2] p3 http://www.hra.nhs.uk/documents/2014/01/cag-meeting-minutes-4-october-2013-2.pdf
[3] http://www.nhs.uk/NHSEngland/thenhs/records/healthrecords/Pages/care-data.aspx
[4] 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

research conduct[5] 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, usable 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 of a new system 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' wellbeing. 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 care.data Privacy Impact Assessment[6]:

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"[7] for academic research, and believe that, if a 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'.

---

[5] World Medical Association Declaration of Helsinki
http://www.wma.net/en/30publications/10policies/b3/

[6] http://www.england.nhs.uk/wp-content/uploads/2014/04/cd-pia.pdf

[7] http://www.adls.ac.uk/wp-content/uploads/ESRC-sensitive-data-secure-rooms.pdf

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 to rigorous independent ethical review and/or have the specific query or queries they want to run on the database scrutinised by an independent body of experts which can assess their likely outcome. If approved, queries may be run but before any significant aggregation of data is permitted to 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 to mitigate risk, 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?[8] 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[9].

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.

[8] https://www.google.com/search?q=nick+clegg+wife+election+elbow+broken
[9] http://www.youtube.com/watch?v=N4HTHyduQzE

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.

In February 2014 we submitted a 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[10]. We noted that there seems to be no requirement to report privacy incidents involving HES data and are sceptical of claims that no privacy breach has occurred[11], 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.

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 only some of the information we asked for in our FOI request, which - given sweeping claims made by NHS England officials - covered the period back to the creation of HES in 1989.

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[12]. All accesses by or provision of data to third parties[13] should be fully reported to the public. Experience with the Department for Education's National Pupil Database shows that when usage of other

[10] https://www.whatdotheyknow.com/request/independent_audits_of_hessus_and

[11] We have now received a partial response to the FOI request in (10) that revealed there was in fact at least one known breach of HES data each year from 2009-2012; no information on previous years was provided.

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

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

sensitive datasets become transparent,[14] 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[15], 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".[16]

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.

Phil Booth, medConfidential
coordinator@medconfidential.org
10 April 2014

[14] https://www.whatdotheyknow.com/request/requests_for_access_to_national#incoming-340035
[15] http://www.hscic.gov.uk/daag
[16] http://www.hscic.gov.uk/media/12911/GPES-IAG-Minutes-for-12-September-2013/pdf/GPES_IAG_Minutes_12.09.13.pdf