The Data Standards Authority, Service Standards, APIs, the NHS, and Public Trust

The remit and risks of the Data Standards Authority are broad; in this note we only cover initial substantive issues. APIs for specific access to necessary attributes are better than bulk data sharing, and medConfidential supports the principle of strengthening the service standard and Technology Code of Practice around data use. However, the details matter.[1]

About medConfidential[2]

medConfidential is an independent non-partisan organisation campaigning for confidentiality and consent in health and social care, which seeks to ensure that every flow of data into, across and out of the NHS and care system is *consensual, safe, and transparent*.

Founded in January 2013, medConfidential works with patients and medics, service users and care professionals; draws advice from a network of experts in the fields of health informatics, computer security, law/ethics and privacy; and believes there need be no conflict between good research, good ethics and good medical care. We also engage with data use across Government, as to a first approximation, the data that institutions of state want to copy most is your medical record.

Background on Data in Government

medConfidential has long[3] engaged with GDS[4] over Part 5 of the Digital Economy Act, and the obligations in the law and the Codes of Practice. In short, there are two particular long term deliverables required from the Data Standards Authority:

- A mandatory register of all projects which use those powers;[5]
- Publication of paperwork for those projects (either proactively,[6] or via FOI[7] if not).

All such documents are theoretically available under FOI, but without proactive publication, for any project that receives significant public attention, a 20+ day wait for FOI is unlikely to provide public confidence in the project – or reassurance in GDS. (Plus, when the analogy is extended to the Data Standards Authority, confidence in the official statistical systems of ONS.)

---

[1] Given this is a new bit of GDS/ONS, we include footnotes to references which will provide context.
[2] www.medConfidential.org
[3] https://medconfidential.org/tag/digitaleconomy/
[4] Originally GDS, then DCMS, now back to GDS.
[5] Currently at https://registers.culture.gov.uk/
[6] https://www.gov.uk/government/publications/data-share-pilot-between-hmrc-and-local-authorities-a-to-c
[7] https://www.whatdotheyknow.com/user/sam_from_medconfidential

DSA staff may benefit from a conversation with the DEA part of GDS – assuming that has not already happened – as the DSA already appears to be repeating some of the missteps of DEA...

Data in the Service Standard and Code of Practice

Requirement: **Will the Data Standards Authority have *lower* standards than the Digital Economy Act Code of Practice?** Replicating the requirement for the Digital Economy Act register, any and every use of an agreement that involves personal data under the auspices of the Data Standards Authority must also be listed in a register. **If such data sharing is <u>not</u> included in a public register, it should not be deemed to have met the standards and norms of ONS / GDS.**

What obligations, if any, are there on the Data Standards Authority (or on ONS / GDS) that provide for secret data agreements based on their work? Excepting a clear and specfic statutory basis, the Technology Code of Practice should be amended to explicitly prohibit data agreements that are not published.[8]

It is unlikely that the most problematic projects will follow the Service Standard (which isn't binding) or the Technology Code of Practice – which arguably is binding, but which is worded so as to have loopholes. The areas of most concern will likely arise around policy-based evidence-making in 10ds, or the "Integrated Data Platform (IDP) for government".[9]

Without complete transparency around projects agreed by the Data Standards Authority, it is not reasonable for GDS / ONS to expect anyone in government – or beyond – to understand the difference between those projects which satisfy the Data Standards Authority, and those which only pretend to be reputable. Otherwise, when politically controversial media firestorms arise, there will simply be no difference in the eyes of the public.

Following the lead of the Office for Statistics Regulation, one fundamental measure the DSA must take to ensure and preserve its institutional integrity is to insist upon publication: something only meets DSA standards *if it is published*.

Similarly, the DSA, the Technology Code of Practice, and all agreements should make explicit that copying data from APIs into local databases *without the explicit consent of the API owner* is prohibited,[10] and cannot be lawful under DPA as a result.

We are aware that demanding high standards of trust and competence will make some Departments run away and hide – the choices ONS / GDS make will drive the behaviours you incentivise. And medConfidential expects to hold GDS/ONS accountable for the outcomes of decisions made.

---

[8] When amending the Technology Code of Practice and Service Standard, it should also be noted that all public services must comply with the Equality Act, and as the Byrom Review notes, without data there is no way for a department or service to assure that it is meeting legal obligations.

[9] https://www.ons.gov.uk/news/news/nationaldatastrategytheonstakescentrestage

[10] https://www.itpro.co.uk/policy-legislation/data-governance/354496/brexit-security-talks-under-threat-after-uk-accused-of - the Home Office breaching data agreements would not be unprecedented...

The standards and outputs of the Audit Trails of API access

Direct care record-finding services in the NHS already have a problem with 'creepy single doctors'[11] looking up the records of patients they go on dates with. What steps the Data Standards Authority will take and require of others to avoid replicating this and related problems across Government are, as yet, unclear.

DWP has already stated to Parliament that it wants access to health and bank records.[12] medConfidential fully expects the most toxic parts of government to be first in line for the most sensitive data.[13]

In an environment of API access to citizens' individual-level data – for the provision of services, etc. – the only viable way to mitigate and detect abuse is for every citizen to know how their data has been accessed via those APIs. If you do not know that your data was accessed, you cannot confirm it was accessed lawfully and properly – nor can you raise questions about whether it wasn't accessed when it should have been.[14]

Without providing this knowledge, GDS / ONS will be advocating intrusion and harms on up to an industrial scale, with no mechanism for detection or redress.

The only meaningful mechanism for detection is for every citizen to be able to know how *their* personal data has been accessed through APIs. There can and should be other systemic checks and safeguards, but for a system to be trustworthy evidence must be provided to the people affected by use of data about them. Fortuitously, with the advent of the forthcoming GOV.UK Login, every government service should be able to show authenticated citizens how data about them has been used, through DSA standardised APIs.

Some work has already been done on what this might look like:

https://medconfidential.org/wp-content/uploads/2015/12/GDUR_web.jpg

[11] https://medconfidential.org/wp-content/uploads/2020/09/Creepy-single-doctors-v2.pdf
[12] Q2, Q3, Q31 – https://committees.parliament.uk/oralevidence/1093/pdf/
[13] There is a reason our report on the data flows in Universal Credit / DWP referenced a Monster Factory
[14] https://medconfidential.org/wp-content/uploads/2020/09/Creepy-single-doctors-v2.pdf

The APIs list[15] – Contents and Remit

The inclusion of the details of NHS direct care[16] APIs in a list of "central and local government" APIs is fundamentally problematic and contrasts badly with the approach that was taken for police APIs, where there is instead a single link to a web page that is hosted within an appropriate domain.

> **For what reason does ONS / GDS think that a government Department might wish to access an individual's direct care End of Life plan?**[17] Or the FGM risk list?[18] Or access any GP medical record in England?[19] Or the details of everyone registered with the NHS?[20] All Summary Care Records?[21] Or prescriptions?[22]

Access to the NHS Personal Demographics Service (PDS) by government Departments is *highly* controversial, and subject to significant governance that goes far beyond mere technical means.[23] [24] [25] [26] It is no longer NHS policy that the Home Office can require any data from the NHS that it deems fit, even if it may be Home Office policy that it can try to do so.

It would be strategically unwise for the Data Standards Authority to persist the mistaken belief that the choices of what it promotes are apolitical, and that data use is 'not our department'.[27]

The choice of the level of detail given for the NHS contrasts starkly (and extremely badly) with the approach chosen for police.uk APIs, where a single api.gov.uk page links users to the relevant information on the police.uk domain. **Why has the approach taken for police APIs not been used for NHS APIs?**

This difference in treatment could be read as a policy decision within the Data Standards Authority that any links which could be made between government and health data, should be available. That is not a GDS decision to take. GDS has neither the knowledge or the expertise to be able to account for the effects of 'monster factories'[28] elsewhere in Government. And more fundamentally, does this mean the position of ONS and GDS is that

---

[15] https://www.api.gov.uk/ or, since the problematic NHS section should get taken down quite quickly: http://web.archive.org/web/20201106203419if_/https://www.api.gov.uk/#uk-government-apis
[16] "direct care" being words with particular meaning in law
[17] https://www.api.gov.uk/nhs/end-of-life-fhir-api/#end-of-life-fhir-api
[18] https://www.api.gov.uk/nhs/female-genital-mutilation-fhir-api/#female-genital-mutilation-fhir-api
[19] https://www.api.gov.uk/nhs/gp-connect-fhir-api/#gp-connect-fhir-api
[20] https://www.api.gov.uk/nhs/personal-demographics-service-fhir-api/
[21] https://www.api.gov.uk/nhs/summary-care-record-fhir-api/#summary-care-record-fhir-api
[22] https://www.api.gov.uk/nhs/prescription-tracker/
[23] https://old.parliament.uk/business/committees/committees-a-z/commons-select/health-committee/inquiries/parliament-2017/mou-data-sharing-nhs-digital-home-office-inquiry-17-19/
[24] https://understandingpatientdata.org.uk/news/health-select-committee-mou-report
[25] https://www.independent.co.uk/news/health/nhs-patient-data-home-office-immigration-enforcement-illegal-asylum-seekers-healthcare-a8186746.html
[26] https://www.theguardian.com/society/2018/may/09/government-to-stop-forcing-nhs-to-share-patients-data-with-home-office
[27] https://www.marketplace.org/2020/10/21/satirist-tom-lehrer-put-his-songs-into-public-domain/
[28] https://medconfidential.org/2020/universal-credit/

any part of Government should in principle have access to any data held elsewhere in Government?

We note one of GDS's private arguments in favour of Chapter 1 of Part 5 of the Digital Economy Act (DEA) was the ability to allow the Home Office access to the medical records of (all) women to "detect" sham marriages.[29] It will come as little surprise that central government has made *zero* use of that Part of the DEA since it became law.[30]

Given its pivotal role in Government data strategy, a great deal of public confidence in data access and data sharing will likely (and probably should) be based on what the Data Sharing Authority does, and also on the transparency with which it does it.

Early signs are not optimistic.

[29] "It is entirely logical for a Home Office official tasked with preventing sham marriages to believe that accessing NHS data that GPs may have on marital happiness would help them do their job. That the Cabinet Office were expecting that to be an example in their public consultation shows how easy it is to misunderstand the public interest. Care.data style mistakes are not an isolated incident in the public sector - it was only the first." - https://publications.parliament.uk/pa/cm201617/cmpublic/digitaleconomy/memo/DEB08.htm

"For example, prior to passage of the Digital Economy Act, a 'sham marriages objective' was discussed where the then-Director of Data at the Cabinet Office raised with NHSofficials whether the Home Office could access all women's medical records, looking for indicators of 'sexual dissatisfaction' to help further this Home Office policy – the narrow objective of one politically-prioritised civil servant." - https://medconfidential.org/wp-content/uploads/2020/09/OKRs.pdf

[30] https://medconfidential.org/2020/data-misuse-as-missed-use/