Defenddigitalme submission to the NDG consultation

About defenddigitalme and what we do

We are a non partisan civil society organisation. We campaign for safe, transparent and fair use of personal confidential data across the education sector in England and beyond. We are funded 2017-19 through an annual grant from the Joseph Rowntree Reform Trust Ltd.

Priority 1: Encouraging access and control, individuals and their health and care data

Greater transparency for patients to see tailored information showing how data about them has been used for reasons other than their own individual care.

Q3. What we would like the National Data Guardian to do in this area:

1. Summary:

- Prioritise children's safe, fair and transparent health data processing across the public sector, not only within NHS.
- Require public documentation and audit of commercial companies that process health data where it is used in- or outside an NHS body and in particular for linkage with other datasets.
- Enforce pro-active communication to children and their families, not privacy notices.
- Encourage data usage reports to demonstrate to children how data are used.
- Restore the balance of common law of confidentiality above commercial interests.
- Prioritise human rights in a world increasingly dominated by demands of machine learning.
- Enforce lawful consent and control by new parents of babies' data in newborn screening.

Priority 2: Using patient data in innovation: a dialogue with the public

How do patients want and expect data about them to be used in health technology? Is there understood to be a reciprocal relationship, whereby those receiving care allow data usage to facilitate improvements? What are the boundaries that people would put around this? Should use of patient data in innovation be one of the NDG's top priorities?

2. The recommendation of the 2014 Science and technology Committee Report, "Responsible Use of Data" should be a priority; "*the Government has a clear responsibility to explain to the public how personal data is being used*."[1] It has both a legal and moral obligation to do so.

[1] https://publications.parliament.uk/pa/cm201415/cmselect/cmsctech/245/245.pdf

3. Government must accept that telling people alone how data are used, nor changing the law, does not automatically confer public favour, or legitimacy for expanding plans on use, and boundaries on this.

4. We refer to the UK Supreme Court decision Christian Institute & Others[2] which concluded that the broad data sharing with third parties in the Named Persons plans and drafted legislation, did, '*not meet the article 8 criterion of being "in accordance with the law".*

5. This has significant implications for bodies that already share children's health data in England, in a similar way and with similar bodies and for similar purposes as was intended in Scotland, and that should rein in, not encourage, even more broad children's data sharing without informed consent.

- Lack of safeguards which would enable the proportionality of an interference with article 8 rights to be adequately examined, where a test is only of desirability of use or data 'user need.'
- Disclosure to a wide range of public authorities without either the child or young person or her parents being aware of the interference with their article 8 rights, and in circumstances in which there was no objectively compelling reason for the failure to ascertain and have regard to their views.
- Failure to inform the parents of a child about the sharing of information.
- Registers of use, while important, cannot replace the active duty to inform, because such a record will not assist a child, young person or parent who is not informed that the information is to be or has been shared, or of the rationale behind a decision to share information.
- Information must be provided in accordance with Article 12 of the UNCRC, "so far as reasonably practicable to ascertain and have regard to the views of the child or young person"

6. While a significant step in enabling more patient control over data was taken in 2018 with the launch of the National Data Opt-out, it did not take children into proper account nor meet public expectations. This was thoroughly documented by medConfidential[3] and needs improvement.

7. How patients expect data about them to be used within health research and its boundaries, was explored in 2016 at length across the UK for the Administrative Data Research Network (ADRN). As part of the work that went into establishing the centres, our funders, the Economic and Social Research Council (ESRC) and IPSOS Mori ran a series of data dialogues to understand the public perceptions and attitudes about the use of administrative data for research.

8. Note this was not for identifying, but de-identified data re-use. One could imagine that for identifying data, the sensitivities would be even greater. Work identified red lines and "*further public dialogue would be needed for any expansion of the ADRN's remit, in particular with relation to:*

- *Creating large databases containing many variables/data from a large number of public sector sources.*
- *Allowing administrative data to be linked with business data*
- *Linking of passively collected administrative data, in particular geo-location data"*

[2] "Named Persons" Supreme Court ruling (2016) https://www.supremecourt.uk/cases/docs/uksc-2015-0216-judgment.pdf para 84 and 85
[3] medConfidential, The Opt out Process for those with Children (November 2018) https://medconfidential.org/2018/children/

9. Unconnected work was done in workshops with young people in 2010, by the Royal Academy of Engineering and others, presented in the report, *Privacy and Prejudice: Young people's views on the development and use of Electronic Patient Record.*[4]

For young people to be in control, or at least have the option to be so, requires a system that will allow them to:

- *have access to own their record; thave a say as to who else gets access to their record and for what purposes;*
- *be assured of privacy from certain groups (for example, parents and potential employers);*
- *make informed decisions by being kept fully up to date about EPR system developments, data security and safety, who gets access and for what purposes in addition to what the implications might be.*

10. It was also felt important that young people be allowed *"to change their minds over time regarding whether to be part of the database, and their privacy settings."*

11. In 2015, Mark Davies said at an NIB meeting, "we have only a sense" and we don't have "a really solid evidence base" of what the public want. He said, "people feel slightly uncomfortable about data being used for commercial gain." Which he said he felt was "awkward" as commercial companies included pharma working for public good.[5]

12. In NHS England's own care.data listening feedback, there was much more than 'a sense'. People were strongly against commercial exploitation of data. Many were livid about its use, [see other care.data event notes[6]] not 'slightly uncomfortable.' And they were able to make a clear distinction between uses by commercial companies they felt in the public interest, such as bona fide pharma research and the differences with consumer market research, even if by the same company.

13. The conflation of purposes of secondary uses remains morally troubling, and will remain practically and lawfully problematic, until NHS England and government design rights-respecting systems, that ensure privacy and data protection by design and default[7] behind the scenes.

14. As medConfidential rightly pointed out[8], risk stratification and commissioning for example, do not need and should not have according to the 2013 Caldicott Review,[9] fully identifiable individual level data sharing. Scope creep in recent years has seen an explosion of processing of health data by non-registered and regulated health and social care professionals.

15. That institutions to continue to disregard this, not only continues to place themselves at reputational risk, but undermines any sense that there is seriousness of intent to do the right thing. Debate on ethics from various parties, continues to be nothing more than window dressing. Perhaps

[4] This study was conducted by The Royal Academy of Engineering (the Academy) and Laura Grant Associates and was made possible by a partnership with theY Touring Theatre Company, support from Central YMCA, and funding from the Wellcome Trust and three of the Research Councils (Engineering and Physical and Sciences Research Council; Economic and Social Research Council and Medical Research Council). https://www.raeng.org.uk/publications/reports/privacy-and-prejudice-views
[5] care.data notes https://jenpersson.com/reputational-risk-caredata-public-confidence/
[6] care.data notes on communications jenpersson.com/care-data-communications-change/
[7] As required under GDPR Article 25
[8] https://medconfidential.org/wp-content/uploads/2015/01/2015-01-14riskstratification.pdf
[9] https://www.gov.uk/government/publications/the-information-governance-review

judicial action in the near future, will be the only way for rights to become enforced and for public sector held personal data to be treated properly.

16. However, the public attitudes towards re-use of their confidential health data, reflected across a decade of research and public opinion polls, is clear and consistent. For leadership to continue to deny this is simply because the answers they receive, are not those they want to hear, or choose to act on.

17. Using technology is commendable to inform patients how their data are used, but apps will not solve embedded bad practice.

18. For public expectations of data usage to match reality, current re-use of data must first become transparent to the public, and use should be focussed on processing by those who have a transparent legitimate relationship with the individual. Uses beyond this are often not what people expect. Bodies such as Public Health England continue to knowingly ignore both fundamental legal and moral obligations in this regards of secondary re-use of data, from cradle[10] to grave. Communications on vaccinations in schools, and the National Child Measurement Programme, fail to mention national data transfer, and secondary data reuses. The National Data Guardian should audit national patient data sharing templates and guidance provided by bodies at national level, and demand regional communications of revised policies.

Priority 2: Using patient data in innovation: public dialogue

19. The 2016 NDG review recommended "*The case for data sharing still needs to be made to the public, and all health, social care, research and public organisations should share responsibility for making that case*".

We disagree with this premise. The case has been made a number of times since 2007, and unlike some parliamentary procedures, it appears that the same argument is allowed to be brought back over and over again. The continued efforts to override the age-old duty of professional confidentiality between physician and patient, and the right to privacy and family life, is a waste of resources that could be more fruitfully spent on effective communication s and consent mechanisms, modern data infrastructure and privacy preserving processing.

20. The confidentiality of health data, is recognised by its status in data protection law as special category data, and means that it is for anyone or organisation that wishes to infringe that right, to respect not make a case to workaround.

21. For processing data which carries an a priori fundamental right to privacy by design and default, it there may be a case to be made for technology solutions that enable non-intrusive use -- such as synthetic data and other privacy respecting technology at source, but lack of funding or unwillingness on the part of the State should not be sufficient case, to walk over individuals' rights in both a legislative and moral perspectives and infringe on the right by default.

[10] Response to the Consultation:NHS Newborn Blood Spot Screening Programme 2017-18 https://defenddigitalme.com/wp-content/uploads/2016/09/DDM_Newborn_Screening_Consultation2509.pdf

22. It has been a deliberate choice at NHS England, exemplified in care.data, to not inform patients fully how data are used. This has not changed since the GPES group in 2013, had *"major concerns about the process for making most patients aware of the contents of the leaflets before data extraction for care.data commenced".*[11]

23. The rhetoric that patients should be in control over their data, seems increasingly to be shorthand for 'let's offer patients pay for privacy' which would exploit the most vulnerable, in the worst way.[12]

24. In response to questions four: The economic arguments of the current capitalist surveillance model dominating debate in the UK public sector, purposefully supported by leaders and former leaders of commercial companies now in public sector and policy influencing positions, must not be supported to put the wants of profit and machine learning, ahead of human rights. That will ensure long term damage to public trust and harm both the long term outlook for continued data collection at scale, and sustainable economic models.

25. The sustainable model for data management is not, as Mr Kelsey wanted in 2013, to "reach out to the customer"[13] but to continue to respect the patient as a person. Although he said care.data would 'respect their privacy' and be with their consent' the reality was neither were true.

26. Priority 3, data in the delivery of direct clinical care. should certainly be the focus of any data processing since that is the purpose of the data collected from interactions with the State healthcare system, and sets the fundamental basis and boundaries for lawful processing.

Linked datasets using Health and Children's social care data

27. What the NHS does with large linked lifetime integrated datasets gets copied by others. We note medConfidential's recent evidence to the Work and Pensions Committee on the wider implications of confidence breaches in health data, and see similar consequences in our work.

28. Since children's social care lies outside the remit of the National Data Guardian it is outwith the scope of this consultation. However, or the record we would like to include a reference to the work of the Data Justice Lab in Cardiff University,[14] which highlights some of the most egregious infringements of confidentiality, and human rights to privacy and protection from intrusion into family life using linked NHS healthcare data, together with and to create data for, social care and inferred risk scores.

[11] GPES group concerns on care.data lack of public and professional communications plan (2013) https://digital.nhs.uk/media/12911/GPES-IAG-Minutes-12-September-2013/pdf/GPES_IAG_Minutes_12.09.13.pdf
[12] Unlocking digital competition, Report of the Digital Competition Expert Panel https://www.gov.uk/government/publications/unlocking-digital-competition-report-of-the-digital-competition-expert-panel An independent report on the state of competition in digital markets, with proposals to boost competition and innovation for the benefit of consumers and businesses.
[13] ibid.
[14] Project Report: Lina Dencik, Arne Hintz, Joanna Redden & Harry WarneData Justice Lab, Cardiff University, UK (December 2018) https://datajustice.files.wordpress.com/2018/12/data-scores-as-governance-project-report2.pdf

Annex: Children's safeguarding

29. We would like the scope of the National Data Guardian's remit to include children's health data regardless of where it is created or processed in the public sector, or as a result of a statutory basis or provision of such services, since unexpected use of these data may jeopardise trust in NHS data use.

30. The exceptions and overrides in the 2016-17 *National Data Guardian Review of data security, consent and opt-outs*[15] included a mention that "**information must be shared for child or vulnerable adult safeguarding purposes."**

31. We would like the consultation to consider that the term safeguarding has become a very broad concept used within children's data across the public sector, and in particular there has been a significant scope creep in its meaning since 2015. We ask that great care is made in using this language, since it could imply that fewer limitations or considerations of due diligence might apply because data '*must'* be shared if the purposes use the language of 'safeguarding'.

32. Department for Education 2018 Statutory Guidance, *Keeping Children Safe in Education (KCSiE)*, [16] includes the Prevent duty as part of safeguarding: "*The Prevent duty should be seen as part of schools' and colleges' wider safeguarding obligations.*" [17]

33. The software used in the monitoring of this policy and practice create and capture health data in education. Mental health, physical health and inferred health related data are captured by a range of commercial companies Internet monitoring software. These are not considered NHS data, but neither are they considered part of the educational record. They sit in no man's land without oversight.

34. The Prevent duty purposes are unrelated to health, and are open to broad interpretation, but may result in the creation and sharing of health data and passing it onwards into the NHS from third parties.

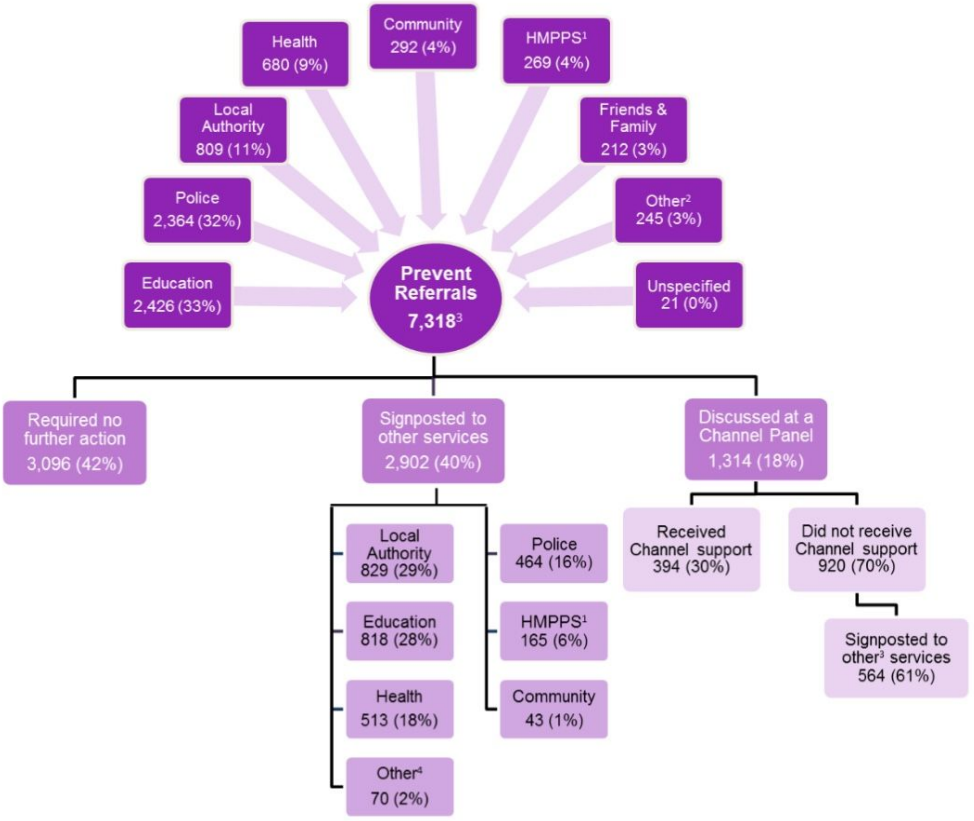
35. That 1/3rd of referrals into the programme come from the education sector, but that over 70% of referrals are deemed not to require any action at all, by police at the Channel panel stage, may indicates a tendency to over refer and *over* not *under* data share, where the staff are uncertain.

36. Of the 40% who are referred, 18% go on to NHS services. More transparency needs encouraged.

37. The multi-agency safeguarding hub data sharing after this referrals process is completely opaque both to participants, and to civil society since Freedom of Information requests have been declined. We address this "chronic lack of transparency" as found by the Child Rights Network in 2016, regards how [health] data are used from and within this process in a the Spring 2019 ICO FOI consultation.[18]

[15] 2016-17 Review of data security, consent and opt-outs Para 3.2.40 p34
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/535024/data-security-review.PDF
[16] Ibid p83
[17] September 2018 DfE Guidance Keeping Children Safe in Education
https://defenddigitalme.com/wp-content/uploads/2018/12/Keeping_Children_Safe_in_Education__3_September_2018_14.09.18.pdf
[18] Defenddigitalme response to the ICO Freedom of Information consultation (March 2019)
https://defenddigitalme.com/wp-content/uploads/2019/03/ICO-FOI-consultation-defenddigitalme.pdf

Figure 3.1: Sector of referral and subsequent journey, 2017/18



Source: Table P.01-02, *Home Office*

DATA PROCESSING FLOW

March 2019