Health & Social Care Information Centre

Trevelyan Square
Leeds
LS1 6AE
Tel: 0300 303 5678
enquiries@hscic.gov.uk
www.hscic.gov.uk

NIC-36407-H5J8Q

1 June 2016

MedConfidential
samsmithsemail@gmail.com

Dear Phil and Sam

Thank you for your letter dated 16th May 2016.

A common understanding of language and meaning in this area is so important and it may be helpful to be clear what we mean when we talk about anonymisation or anonymised data. It is probably most helpful to draw on the ICO code of practice[1] as this is an authoritative source of good practice. Anonymisation is defined in the code of practice as a broad term that covers techniques used to convert personal data to anonymised data e.g. by aggregating the data so that it could then be published or applying a pseudonym to patient level data for a more restricted use. The intent of anonymisation is to turn data into a form which does not identify individuals and where identification through its combination with other data is not likely to take place. In this sense anonymised data is not patient identifiable information. It is also worth noting that "anonymised" data is distinct from "anonymous" data i.e. data from which an individual could never be re-identified and, therefore, anonymous is not an appropriate term to use in this context.

The ICO code of practice makes a further important distinction between publication to the world at large and the disclosure on a more limited basis – for example to a particular research establishment with specific conditions attached. The latter may present a greater privacy risk, but these risks are controlled, e.g. limiting who has access to the data, restrictions on usage and prohibiting further disclosure.

The ICO confirms the position that the Data Protection Act (DPA) does not require anonymisation to be completely risk free, rather that these risks are controlled and managed. The code recognises a distinction between providing anonymised data to the public at large and providing anonymised data for limited access and Chapter 7 describes a set of 12 key safeguards to be considered when releasing anonymised data for limited access. As such, data controllers are required to take a risk based approach in balancing the risk of re-identification with the controls in place.

The HSCIC policy position is that type 2 opt-outs do not apply where direct identifiers in the data sets have been removed or replaced with pseudonyms; and the data dissemination application has been approved for release through the end to end Data Access Request Service (DARS). This includes the request being recommended for approval by the Data Access Advisory Group

[1] ICO Anonymisation: managing data protection risk code of practice

(DAAG), or in the future the Independent Group Advising on the Release of Data (IGARD). In such cases the Data Sharing Framework Contract (DSFC) in combination with the Data Sharing Agreement (DSA) set out terms and conditions which go above and beyond the 12 safeguards set out in the ICO code of practice. To be absolutely clear re-identification of anonymised data, unless this is specifically agreed in the DSA for an agreed purpose, would be a breach of contract. Such an event would also trigger a Data Protection Act breach via principle 1 i.e. processing data fairly and lawfully.

Where health and social care information about a person, or about a population of people, is first anonymised, no lawful basis for the dissemination is required. Such data are disseminated using HSCIC powers under the Health and Social Care Act 2012. As long as individuals will not be identified by the recipient(s), the data may be published or provided to specific organisations or people. Patient identifiable information always requires a specific legal basis for its disclosure; The Data Release Register includes information on both types of data release.

This risk-based approach allows us to make information derived from personal data available in a form that is rich and usable, whilst protecting individual data subjects. This approach has a number of wider benefits, e.g. enabling the development of new treatments to improving health and care services. This approach conforms to the spirit and letter of the Secretary of State's Direction re processing Type 2 objections, ICO Undertaking to comply with the Data Protection Act 1998, legal and regulatory frameworks.

With regard to your point about potentially commercial purposes there are two points to make. Firstly, when we publish information we have no control over who might use it and how it is used. We do not apply opt-outs to data which we publish. Secondly for data disseminations, data purposes are considered as part of the DARS process including an independent assessment by DAAG/IGARD in conformance with Section 122 of the Care Act 2014 i.e. data would not be disseminated for purely commercial purposes and must be for the benefit of health and care.

I can confirm that the Data Release Register planned for August, which will cover the period April 2016 to June 2016, will show for each data release whether type 2 opt-outs have been applied and the reason for that decision. I am keen to work with you in terms of the ways in which our Data Release Register and fair processing materials can be improved and made clearer to the public and would be happy to consider any other suggestions you might have to improve the materials published so far. As Kingsley set out in his letter to you, we recognise that there is more to do in this area which we all know is technically complex and therefore it is important to us that we communicate this as clearly as possible.

Yours sincerely

Martin Severs
Interim Executive Director of Information & Analytics, Medical Director and Caldicott Guardian

cc Sir Nick Partridge, Non-Executive Director, HSCIC
Dame Fiona Caldicott, National Data Guardian
Andy Williams, Chief Executive Officer, HSCIC