Information Commissioner's Office

Upholding information rights

Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF
Tel. 0303 123 1113 Fax. 01625 524 510 www.ico.org.uk

Phil Booth
Sam Smith
MedConfidential

By email only to coordinator@medconfidential.org

22 November 2016

Dear Phil and Sam

Re: Complaint about objections to dissemination of data from the HSCIC (now NHS Digital)

Thank you for your letter to the Information Commissioner of 7 July, and subsequent correspondence and contact, in which you set out your concerns about NHS Digital's dissemination of Hospital Episode Statistics (HES) data and how this implements the ICO undertaking signed by NHS Digital on 19 April 2016.[1]

I understand your main concern to be that NHS Digital's implementation and handling of HES is not sufficiently "anonymised" according to the intent and meaning of the ICO's "Anonymisation: managing data protection risk code of practice"[2] and other standards. This is particularly relevant because the undertaking, by which NHS Digital committed to implement Type 2 objections, provides that such objections do not have to be implemented where data is anonymised in accordance with the ICO's code.

I have made enquiries of NHS Digital and they have confirmed that requests for data are dealt with via the Data Access Request Service (DARS) which assesses, amongst other things, the nature of the data requested, the purpose for which it has been requested, the security of applicants' data handling and storage systems. Where the data to be disseminated needs to be anonymised, NHS Digital replaces direct identifiers with a pseudonymised identifier, which is encrypted with a different encryption key for each purpose. Even if this encryption is broken, NHS Digital is satisfied that there is "no way of referring back to the original identifiers from the unencrypted data without the use of the lookup table which is not available outside NHS Digital." This addresses the risk of re-identification directly from the data itself.

However, you correctly point out that re-identification can also take place indirectly, from the data disclosed in combination with data already in the possession, or likely to come into the possession of, the recipient. To address this risk NHS Digital releases data under specific terms and conditions, enforced by a data sharing agreement (DSA)

[1] https://ico.org.uk/action-weve-taken/enforcement/health-and-social-care-information-centre-hscic/
[2] https://ico.org.uk/media/for-organisations/documents/1061/anonymisation-code.pdf

underpinned by a contract. We understand that these terms include:

- A clear requirement in the DSA that data is processed only in accordance with the specific purpose set out in the DSA. This is reiterated in the contract.
- Prohibition (in the contract) of linkage with any data held by the recipient unless that linkage has been expressly included within the approved application.
- Prohibition in the contract of any manipulation or use of the data in any way that would re-identify any individual.
- Requirement that the data must be kept separate from all other data, unless otherwise has been agreed as part of the application.
- Any onward sharing of the data is prohibited in the contract unless prior approval has been obtained from NHS Digital.
- Requirements in the contract to appropriately vet staff who will have access to the data.
- Requirements in the contract around appropriate technical and organisational security, of which the recipient is required to provide explicit evidence.
- The DSA specifies the length of time approval is in place for and the contract requires the permanent destruction of the data at that time, with the submission of a certificate of destruction as proof.

There are a number of sanctions in place should any recipient breach the terms of the contract or DSA, which include immediate termination of the agreement, plus a requirement to report any breach via the IG Toolkit's Serious Incidents Requiring Investigation reporting tool, or direct to the ICO.

In addition, the contract also gives NHS Digital the right to audit recipients. An annual programme is in place, supplemented with audits where there is a concern about data handling, and all reports are published on NHS Digital's website.

In summary, NHS Digital has implemented controls and safeguards that correspond with the safeguards set out in chapter seven of the ICO anonymisation code. As to whether this will be sufficient to reduce the risk of re-identification below reasonable likelihood will depend on the particular circumstances of any application and subsequent data release. Our Anonymisation code of practice states that "It should be noted a pre-defined list of risk mitigations cannot be exhaustive. Data controllers must conduct their own risk assessment, eg using their organisation's normal data security risk assessment processes. Co-ordination between the organisations involved in a project should help to identify other security measures that may need to be included."[3]

Whether a data release can be appropriately deemed anonymised to the extent that the risk of re-identification is reduced to "not reasonably likely" will depend on the data

[3] https://ico.org.uk/media/for-organisations/documents/1061/anonymisation-code.pdf

released, and the contractual terms and other controls put in place. Depending on the data and the recipient's data handling arrangements it may be appropriate to consider other security measures to ensure that the risk of re-identification remains acceptably low. NHS Digital should ensure that the DARS process incorporates an appropriate assessment to enable a decision to be made as to whether further measures are required.

We note that where a data request is for more of the same non-identifiable data, or to hold the same non-identifiable data for longer, there is no requirement for the application to be re-submitted to the Data Access Advisory Group, but that the Information Asset Owner and Director for Data Dissemination must be satisfied that the data is still not reasonably likely to identify individuals. We would comment that it is very important that an assessment is carried out to ascertain that this is still the case, especially in the light of any changes that may have taken place in the arrangements under which that data, and other data, are held by the recipient.

We would also expect NHS Digital to carry out periodic reviews of their policy on the release of data and the anonymisation techniques they use, based on current and foreseeable threats, and to undertake testing the effectiveness of their anonymisation techniques.

Whilst I will write to NHS Digital to inform them of our views in this matter, I should point out that the ICO has not received any complaints that recent HES data releases have disclosed personal data when the release purported to be anonymised. Of course, if we were to receive any specific concerns in this regard we would investigate the matter further.

Yours sincerely

Victoria Cetinkaya
Senior Policy Officer (Public Services)