



Health & Social Care
Information Centre

Health and Social Care Information Centre

Information Governance Assessment

Customer: NHS England – *care.data* addendum

Customer Requirement Reference Number: NIC-178106-MLSWX.A0913

Date: 29/08/2013

Version: v1.0

1 Information Governance Assessment summary sheet

Customer requirement reference	NIC-178106-MLSWX.A0913
Customer organisation(s)	NHS England
Data controller (if different)	HSCIC
Purpose classification	Secondary purposes
Aggregated or individual-level data?	Both
Identifying or non-identifying?	Not assessed in this addendum
Legal basis (if identifying)	

IG Assessor comments

For an explanation of the entries for "identifying or non-identifying" and "data controller" above, see section 2.1.

Assessed by M Oswald

The information governance assessment of the addendum follows overleaf.

2 Information Governance Assessment

2.1 Introduction

This information governance assessment is not assessing a full GPES extraction, but an addendum to a previously-assessed and agreed extraction: care.data. The original proposal involved extracting identifying data from general practice records, in order to link the data to other data sources, and make available in pseudonymised form to NHS commissioners, and also publish data once anonymised. The data to be released by the HSCIC would not identify patients.

This information governance assessment assesses a proposed change to the original requirement: to extend the range of data recipients beyond commissioners. NHS England proposes that any organisation or person should be able to receive the pseudonymised data as long as they are approved under HSCIC governance procedures.

2.1.1 Identifying or non-identifying?

The information governance assessment for the care.data extraction in March 2013 assessed the extraction to be identifying as patient identifiers such as NHS Number were being extracted from general practice systems, stored, and processed by the HSCIC. The requirement was that the patient data were then either aggregated and stripped of small cells and published, or made available to commissioners after a process of pseudonymisation (i.e. removing identifiers like NHS Number and replacing them with a unique meaningless pseudonym). This assessment concerns only the addendum to that original extraction: the proposal to change the potential recipients of the pseudonymised data, widening the range of future recipients beyond commissioners. This information governance assessment of the addendum is not classified in the summary sheet as either identifying or non-identifying because no assessment is made, or can reliably be made, of all of the possible additional disclosures of data to the wide variety of recipients that could result from this proposal. However, the clear intent of NHS England and the HSCIC is that this addendum proposes only the release of non-identifying data.

2.1.2 Data controller

The Health and Social Care Information Centre is a data controller for the personal data extracted through GPES and linked to other datasets. The HSCIC determines how those data are processed. The HSCIC is responding here to requirements set out by NHS England, and so the two organisations might be considered to be joint data controllers. However, the Information Commissioner's Office has advised that the HSCIC should be considered the data controller for care.data.

2.1.3 Structure of this information governance assessment

As it is not assessing a standard extraction requirement, this information governance assessment follows a non-standard structure. Section 2.2 assesses the HSCIC's governance procedures for releasing data to outside agencies, and in particular the specific arrangements for pseudonymised data. The HSCIC's governance arrangements were examined in the original care.data information governance

assessment. However, the balance of risk and benefit changes when the data recipients change, and their uses of the data change. For example, it may be justifiable to find a governance process acceptable when releasing pseudonymised data to commissioners (which may be low risk, high benefit) and not acceptable for other recipients. Therefore, the governance process merits re-examination here in section 2.2.

Section 2.3 assesses the proposal from NHS England to extend the range of data recipients in the light of these governance arrangements.

2.2 HSCIC governance of the data disclosures

The HSCIC governance arrangements described in the addendum to the customer requirement summary provide a systematic approach that must always be followed before data are released to external agencies. Organisations requesting data have to give evidence of proper information governance arrangements (for example, their assessment scores under the Information Governance Toolkit). Data recipients commit in writing to strict information governance requirements and restrictions, including storing and processing the data securely, not sharing data, and only using data for the agreed purposes. The HSCIC data sharing agreement with data recipients is currently subject to change, and will be published shortly.

Data requests will be classified according to whether or not they contain any “personal confidential data”¹. The requests are classified as to whether they are identifying or non-identifying according to the data required; given the volume of requests, it is considered impracticable to assess each one individually. Personal confidential data requests (i.e. identifying data) are outside the scope of the current care.data extraction for GPES. All other requests must be approved by the person(s) responsible for the dataset(s) (the “information asset owners”), who may seek advice from HSCIC information governance staff. Requests for non-personal confidential data that include data items classified as “sensitive”² must also be approved by the Data Access Advisory Group (DAAG). DAAG contains a mixture of HSCIC and external staff³. Minutes of DAAG meetings are published.

The HSCIC website publishes details about this process, and provides examples of the kinds of organisations and the kinds of uses to which the data are put. No rules are published as to which types of organisation are acceptable as data recipients and which organisation types are not acceptable. However, pseudonymised data are only ever released to organisations planning to use the data for purposes concerned

¹ This classification is done on the basis of whether the request contains any of the data items listed as identifiable, namely: NHS Number, Date of birth, or Postcode. See http://www.hscic.gov.uk/media/12072/PID-and-Sensitive-Fields-HES-and-MHMDSv1110613/pdf/pid_and_sensitive_fields_hes_mhmds_v1_110613.pdf

² “Sensitive” data items are a combination of items of health information that are considered especially sensitive (such as the legal status of a person detained under the Mental Health Act), and items that identify the clinicians involved in the patient’s care (such as the consultant code). See: http://www.hscic.gov.uk/media/12072/PID-and-Sensitive-Fields-HES-and-MHMDSv1110613/pdf/pid_and_sensitive_fields_hes_mhmds_v1_110613.pdf

³ See: <http://www.hscic.gov.uk/daag>

with health and social care. The details of all of the data recipients and their uses are not published. Such data have been requested under the Freedom of Information Act, but the requests were found to be exempt under the Act on the grounds that the data are commercial in confidence. However, it is proposed that a register of all bodies requesting data from the Care Episode Service linked data set under care.data, and a brief statement of the purposes to which they will put the data, will be published by the HSCIC. Purposes are to fit within one of the categories set out in the Customer Request Summary addendum.

In summary, access to data is tightly controlled. Although data requests are not subject to scrutiny by people from outside the HSCIC (as required under the GPES IG Principles), and the governance arrangements do not provide the same degree of transparency and fair processing information as GPES, organisations receiving data must commit to stringent requirements to protect the data received. Unlike GPES where requests are individually assessed, the HSCIC arrangements provide for standard datasets of pseudonymised data that have been classified as non-identifying on the basis of their contents to be made available to approved organisations that sign the data sharing agreement. Privacy breaches are liable to result in sanctions from the Information Commissioner's Office.

2.3 The proposal to increase the range of data recipients

2.3.1 Is the proposal acceptable in principle?

Many members of the public see a great difference between public and private uses of medical records, and between uses that are in the interests of good healthcare and other uses⁴. For some people, using medical records for private profit without the explicit consent of individuals is simply wrong.

However, there is no legal requirement to differentiate between the release of data to NHS commissioners and any other potential data recipient. In the eyes of the law, a government department, a university researcher, a pharmaceutical company, or an insurance company is as entitled to request and receive de-identified data for limited access as a clinical commissioning group, as long as the risk that a person will be re-identified from the data is very low or negligible. Furthermore, all such organisations can make good use of the data. Access to such data can stimulate ground-breaking research, generate employment in the nation's biotechnology industry, and enable insurance companies to accurately calculate actuarial risk so as to offer fair premiums to its customers. Such outcomes are an important aim of Open Data⁵, an important government policy initiative.

⁴ See, for example, pages 65-67 of the Demos survey report at: http://www.demos.co.uk/files/Private_Lives_-_web.pdf, and section 5.8 of *Privacy and prejudice: young people's views on the development and use of electronic patient records*, available at: http://www.raeng.org.uk/news/publications/list/reports/Privacy_and_Prejudice_EPR_views.pdf

⁵ See <http://data.gov.uk/>

2.3.2 The impact on the risk / benefit balance

The proposal to extend the range of recipients of data extracted through care.data changes the risk/benefit balance. New benefits are available, but these have to be weighed against the risks that result from supplying pseudonymised data to a much wider range of potential recipients. The extent of those risks has to be considered in light of the proposed governance arrangements outlined in section 2.2 above.

Care.data is a new initiative, and relatively few people are aware of it, or of how data from their GP records will be extracted, linked to their hospital records, and used. NHS England and the HSCIC are beginning to address this with publicity materials, including patient leaflets (some about to be published) which have been developed in conjunction with the Information Commissioner's Office. Materials published so far do not explain in detail plans to make available pseudonymised patient-level data to a variety of private and public organisations. A privacy impact assessment for the HSCIC is due to be published shortly. It mentions care.data explicitly and identifies the normal governance arrangements and controls adopted by HSCIC when processing applications for data. A privacy impact assessment about the use of GP data for care.data is being produced by NHS England, and this offers an opportunity to carry out wider public consultation and to explain the risks as well as the important benefits of care.data.⁶

Note that patient objections to the release of identifiable data by the HSCIC are not relevant here because the data being released are not identifiable.

2.4 Conclusions

Extending the range of recipients of care.data introduces new benefits and risks. HSCIC governance arrangements tightly control the release of data, although these are open to limited external input or scrutiny. Data recipients do make important commitments to protect the data they receive, though this is not currently backed by any routine external audit or accreditation scheme. Opening up valuable data to external agencies is an important government policy, but many members of the public would be uneasy about private companies benefitting from their health data.

The risks associated with the sharing the data of course need to be considered against the benefits to be achieved. Many more organisations will be able to make better use of valuable data offering potential benefits to the public.

⁶ See page 3 of the NHS England bulletin: <http://www.england.nhs.uk/wp-content/uploads/2013/08/ig-bull-2.pdf>

3 Assessors

Assessment made by:

Name: Malcolm Oswald

Role: GPES Information Governance Advisor

Date: 20/08/2013

For the Health and Social Care Information Centre

Assessment checked by:

Name: Clare Sanderson

Role: HSCIC Director - Solution, Design, Standards & Assurance

Date: 20/08/2013

For the Health and Social Care Information Centre

The persons above confirm that to the best of their knowledge the information governance assessment is fair and accurate.

Does either of the two people above have any caveats or other comments to state in relation to the information governance assessment provided?

No
