General Practice Extraction Service (GPES)

Information Governance Principles

Date: February 2014

Introduction

The GPES Information Governance Principles

The confidentiality and security of patient data is of paramount importance to us. GPES has established Information Governance Principles that were approved by the National Information Governance Board (NIGB) and also by the Medical Ethics Committees of the British Medical Association (BMA) and the Royal College of General Practitioners (RCGP).

1 GPES Information Governance Controls

1.1 General principles

1. Before any general practice electronic patient records are accessed, all requests from customers to GPES to run queries to extract data will be:
    a. initially reviewed and refined by GPES staff so that only the minimum necessary data are extracted and passed to customers[1];
    b. classified by the HSCIC as either an "effectively anonymised"[2] or "patient identifiable" data extract, and for either a secondary purpose[3] or for direct patient care, drawing on advice from other bodies as appropriate;
    c. scrutinised and agreed by the Independent Advisory Group (IAG) ensuring through a risk and benefit analysis that the extraction is, in the view of the IAG, appropriate and in the public interest;
    d. authorised by the practice, who will be given fair and sufficient information and reasonable time and choices (see section 3) on whether to participate in queries;
    e. publicised on the HSCIC website[4].
2. All data extracted from a general practice by GPES will be:
    f. stored, processed and transmitted securely;
    g. accessible only through role-based access controls[5] (and with all accesses recorded in audit trails)[6] to:

[1] Note that a customer organisation might request that extracted data are passed to a different organisation.

[2] Whether data are effectively anonymised or patient identifiable is based on a risk assessment that takes account of how, and by whom, the data are to be used. Where the risk of revealing a patient's identity is nil or negligible, data can be considered effectively anonymised. For further explanation, see Annexes A and B of *NHS Confidentiality Code of Practice at https://www.gov.uk/government/publications/confidentiality-nhs-code-of-practice , and the Anonymisation Code of Practice at: http://www.ico.org.uk/for_organisations/data_protection/topic_guides/anonymisation*

[3] A "secondary purpose" is one where the purpose is not direct patient care or individual clinical audit. It includes uses such as health care planning, commissioning of health services, and research. A mechanism has been introduced to capture a patient's preference to be excluded from disclosures of patient identifiable data by general practices for secondary uses; see pages 24-26 of the HSCIC Guide to Confidentiality at: http://www.hscic.gov.uk/media/12822/Guide-to-confidentiality-in-health-and-social-care/pdf/HSCIC-guide-to-confidentiality.pdf

[4] See the customer requirements at: http://www.hscic.gov.uk/article/3472/Customer-requirements

[5] A means of controlling access to IT systems so that what system users can do, and what data they can access, is determined primarily by their job role.

i. the general practices providing the data,

ii. authorised GPES users[7] (contractor and HSCIC personnel), and only where necessary to ensure the data are processed correctly,

h. released to customers when processing is complete, but only where customers have signed a data sharing agreement with the HSCIC stipulating that the data will be stored securely and accessed and used only for agreed purposes and in line with non-disclosure policies[8];

i. deleted from GPES data stores as soon as the data have been released to, and accepted by, customers.

3. A record of the query (but not the query output) and the date(s) it was run will be retained for audit purposes.

4. Although data will be held for only a short period of time, the HSCIC will respond to any requests from patients asking for a copy of the information held about them[9]. Patients are also entitled to ask GPES customers to provide a copy of information held about them.

5. Practices, as data controllers, have a legal responsibility to make patients aware of how their personal data are used for GPES and other purposes, and the choices available to them. A leaflet about information sharing was sent to every household in England in January 2014 including a link to a webpage providing examples of how data may be used including the information extracted using GPES[10].

6. Where GPES is notified that it has received inaccurate personal data[11], GPES will inform the source of the data (the general practice) and the customer (if they have been passed the data). If the customer has not been sent the data, any inaccurate data will be corrected prior to transmission.

---

[6] GPES will be able to provide to a patient on request, a copy of when and by whom GPES was used to access data files currently held by GPES that may contain identifiable data about the patient.

[7] "Authorised GPES users" or "users" are those people with direct access to GPES systems. It excludes systems administrators who may require direct access to GPES data to analyse or solve problems in the way systems are operating. Customers will have separate systems holding data provided by GPES, although some customer representatives will become GPES users so that they can define queries.

[8] Non-disclosure agreements include restrictions on publishing aggregate reports containing small numbers. In addition, customers will be audited periodically for compliance to the terms of agreements.

[9] The Data Protection Act empowers patients to submit a subject access request for a copy of personal data held by an organisation. Effectively anonymised data are excluded.

[10] More information on the fair processing of data can be seen here: http://www.england.nhs.uk/wp-content/uploads/2013/11/cd-fair-pro-guid.pdf

[11] If the notification is not from the general practice, GPES will always confirm with the general practice that data are inaccurate before taking action.

1.2 Controls applicable to different types of GPES queries

7. Note that where the only data recipient for the query is the general practice itself, none of the controls in this section applies.
8. Where all the data extracted from a general practice through GPES are "effectively anonymised" at the time of extraction, or wholly inaccessible by any user until they have been effectively anonymised[12], then:
    a. data covering all patients could be included in queries[13];
    b. customers will be able to use and publish such data for agreed purposes as long as the data remain "effectively anonymised" and within their data sharing agreements with the HSCIC.
9. Where patient identifiable data extracted from a general practice are potentially accessible by authorised GPES users[14] but are then further processed by GPES so that they are only released to, and accessible by, a customer once they are "effectively anonymised", then:
    a. NHS Care Record Service patient choices[15], where adopted by general practice systems, will be respected, so that no restricted information will be extracted;
    b. patient consent, Section 251 approval[16], or statutory justification[17] will be required;

[12] This is to allow for situations where data are extracted in identifiable form but are then processed by software to anonymise that data without giving the opportunity for disclosure to any user. An example of such processing is removing or systematically changing small numbers (e.g. 1s and 2s) in cells in aggregated data that could reveal a person's identity.

[13] The information would not identify patients so patient objections would not apply. This is consistent with the policy of, and interpretation of the law taken by, the Department of Health (see *NHS Confidentiality Code of Practice 2003* page 33).

[14] An "authorised GPES user" is a person (normally an HSCIC staff member) who has been authorised and given access by the HSCIC to GPES computer systems.

[15] The relevant choices with respect to general practice records are dissent to Detailed Care Record sharing (allowing patients to stop confidential information being accessible by external organisations), patient sealing and sealing and locking, and s-flagging. These are methods for patients restricting access to, and disclosure of, their records. Information about these controls is available at: http://www.connectingforhealth.nhs.uk/systemsandservices/infogov/confidentiality.

[16] Section 251 approval is a possible alternative to consent where gaining patient consent is not practicable. See: http://www.hra.nhs.uk/hra-confidentiality-advisory-group/what-is-section-251/. Department of Health policy is that patient consent can be implied where disclosures are for direct patient care, but explicit consent, section 251 approval or another justification in law is required where disclosures are for secondary purposes.

[17] One example is the Health and Social Care Act 2012. Another example is the requirement on general practices to supply confidential information to NHS England in specified circumstances under the *Confidentiality and Disclosure of Information (General Medical Services, Personal Medical Services*

c. where data are extracted for secondary purposes (see section 2.1), no patient data will be extracted if the general practice has recorded a patient's objection[18] to disclosures of patient identifiable data from the general practice for secondary uses even where Section 251 approval has been given (however patient data will be extracted where the disclosure is for direct patient care[19], and may be extracted where required by law);

d. customers will be able to use and publish data received for agreed purposes as long as the data remain "effectively anonymised", and within their data sharing agreements with the HSCIC

10. Where data extracted from a general practice through GPES and released to customers are patient identifiable then:

a. NHS Care Record Service patient choices, where adopted by general practice systems, will be respected, so that no restricted information will be extracted;

b. patient consent, Section 251 approval, or statutory justification will be required;

c. where data are extracted for secondary purposes (see section 2.1), no patient data will be extracted if the general practice has recorded a patient's objection[20] to disclosures of confidential information from the general practice for secondary uses even where Section 251 approval has been given (however patient data will be extracted where the disclosure is for direct patient care, and may be extracted where required by law);

d. customers may disclose these data to other parties:

i. for "medical purposes"[21] where they have a legal basis and where agreed by the IAG and other approval bodies, or

ii. where disclosure is required by law (e.g. in response to a court order).

---

and Alternative Provider Medical Services) Directions 2013 (available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/183372/The_Confidentiality_and_Disclosure_of_Information_Directions_2013.pdf) and the associated code of practice.

[18] See pages 25-26 of the Health and Social Care Information Centre Guide to Confidentiality in Health and Social Care, available at: http://www.hscic.gov.uk/confguideorg and see http://www.england.nhs.uk/wp-content/uploads/2013/08/cd-guide.pdf for the objection codes.

[19] Although note that patients can object to such disclosures for direct patient care through NHS Care Records Service dissent to Detailed Care Record sharing. An example of a query for direct patient care is one where the extract is used to invite patients to participate in a national screening programme.

[20] See pages 25-26 of the Health and Social Care Information Centre Guide to Confidentiality in Health and Social Care, available at: http://www.hscic.gov.uk/confguideorg and see http://www.england.nhs.uk/wp-content/uploads/2013/08/cd-guide.pdf for the objection codes.

[21] As defined in the Data Protection Act 1998 and Health and Social Care Act 2006. It extends beyond direct patient care, and includes, for example, medical research and health care management.

2 General Practice Participation

11. A general practice will be able to change any of its choices at any time. When a query is run, current preferences will be used.
12. This includes an opportunity for general practices to view data extracted and opt out of a query before the data are sent to the customer (see point 16 below for further information).

2.1 Participation in GPES

13. There will be one general choice, supported by a data processing agreement between the HSCIC and the general practice: the general practice will be asked to choose whether or not general practice data may, in general, be extracted for queries outputting "effectively anonymised" data.
14. General practices will not be given a general choice to opt in or out of all queries that extract patient identifiable data; they will be informed about each such query and asked to choose on a query-by-query basis.
15. Where no response is received from a general practice about the general choice above, or about a particular query, GPES will assume “no”[22] and will not extract data.
16. GPES will always respect general practice choices about access to general practice data[23]. It is expected that all general practices will agree to certain essential extracts such as QOF (which is a planned GPES query). Under the Health and Social Care Act 2012, practices may be required to provide identifiable or effectively anonymised information to the HSCIC in such form and manner, and within such period, as the centre may specify[24]. This would empower the HSCIC to require general practices to supply data using GPES for certain extractions. However, where general practices do not wish to use GPES for the extraction, they can agree an alternative method of providing the required data, but it must be acceptable to the HSCIC.

[22] Without explicit general practice agreement, access may be unauthorised and not consistent with the Data Protection Act.

[23] Whether a disclosure is justifiable in the public interest can only be judged by the practice, taking account of both the public interest in favour of disclosure and the public interest in maintaining public trust in a confidential service, alongside the private interests of the individuals concerned.

[24] See sections 254, 255 and 259 of the Health and Social Care Act 2012, available at: http://www.legislation.gov.uk/ukpga/2012/7/enacted. Section 254 of the Act empowers the Secretary of State and NHS England to direct the HSCIC, and section 255 gives other bodies powers to request the HSCIC, to collect information. Section 259 gives the HSCIC powers to require general practices and other health and social care organisations to supply that information (in specific circumstances).

2.2 Opt in or out of specific queries

17. Regardless of their general preference with respect to effectively anonymised queries (see 3.1 above) a general practice may choose a different preference with respect to a particular query[25]. So, even if a general practice has chosen "yes" in relation to effectively anonymised queries, they may choose "no" in relation to a particular query.
18. Before every patient identifiable query is run, general practices will be asked to agree to the extract.

2.3 Notification of queries

19. General practices will be notified about all GPES queries before they are run. The only exception to this is that general practices whose general choice is to allow effectively anonymised queries can subsequently choose to not be notified about each of those queries.
20. The general practice should decide whether they wish to be notified:
    a. before the query is first run or
    b. before every instance of the query being run.

    Where no response is received from a general practice, GPES will assume option b) – before every instance of the query being run.
21. General practices will be able to change their notification preferences at any time. Details of all queries will be published[26] before they are run (after consideration by the IAG). General practices will be able to view, and if necessary revoke, general practice data being output before it is sent to the customer.
22. GPES will always follow a general practice notification preference unless the IAG decides that all general practices should be notified of a query regardless of their preferences. This might happen where the IAG feels there is a particularly strong public interest in running a certain query (e.g. to identify health needs during a pandemic).

[25] A GPES query is software which extracts data which may be run one or more times (each one a "query instance").

[26] See the customer requirements at: http://www.hscic.gov.uk/article/3472/Customer-requirements