



The General Practice Extraction Service Information Governance Principles

The NHS Information Centre is England's central, authoritative source of health and social care information.

Acting as a 'hub' for high quality, national, comparative data, we deliver information for local decision makers, to improve the quality and efficiency of care.

www.ic.nhs.uk

Author: The NHS Information Centre, General Practice Extraction Service

Version: FINAL v1.0

Date of Publication: 01.03.2010

Contents

Foreword	4
Introduction	5
Document Purpose	5
Document Audience	5
Document Status	5
GPES Information Governance Controls	6
General Principles	6
Controls applicable to different types of GPES queries	8
General Practice Participation	10
Participation in GPES	10
Opt in or out of specific queries	10
Notification of queries	11
Document control	12
Reviewers	12

Foreword

General practice records enable doctors to provide their patients with the care they need. But they are also the closest thing that we have in the NHS to a comprehensive lifelong record of a patient's health and the treatment they receive. As such they are a very valuable source of information, providing the potential for the NHS to learn more about the health needs of the population, and how best to address those needs.

The General Practice Extraction Service (GPES) will be able to unlock that potential, but for it to succeed, patients and doctors must trust that the confidentiality of patient records is properly protected. As recent guidance published by the General Medical Council sets out¹:

'Patients have a right to expect that information about them will be held in confidence by their doctors. Confidentiality is central to trust between doctors and patients. Without assurances about confidentiality, patients may be reluctant to give doctors the information they need in order to provide good care'.

The GPES Information Governance Principles paper sets out the commitments proposed by the NHS Information Centre to safeguard the confidentiality of information in patients' records. All requests for information made to GPES will be approved by an Independent Advisory Group which will check conformance to these Principles. A fundamental principle is that information extracted will be anonymised wherever possible. Where this is not possible, a legal justification will be necessary. However, patients who remain concerned despite these safeguards will be able to opt out of GPES.

On behalf of The NHS IC, I welcome the publication of the GPES Information Governance Principles, and the request for feedback from the public and NHS.

¹ See: http://www.gmc-uk.org/guidance/ethical_guidance/confidentiality.asp

Introduction

Document Purpose

The purpose of this document is to set out the main information governance principles and controls underpinning GPES, the General Practice Extraction Service² being designed by the NHS Information Centre. These principles apply to Phase 1 of GPES, where data will be extracted from practices for customers that are national, health-related bodies.

Document Audience

The document is aimed at GPES stakeholders including representatives for patients, the medical profession and general practices. Once approved, this document will be published along with other communication materials to further explain these principles and controls.

Document Status

Following initial consultation, this paper was agreed by the National Information Governance Board at their meeting on 10th September 2009, was amended to reflect subsequent comments, and was then approved by the GPES Delivery Board and GPES Project Board.

² For more information, see <http://www.ic.nhs.uk/gpes>

GPES Information Governance Controls

General Principles

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; and
- b) Classified by the Independent Advisory Group as either an “effectively anonymised”³ or “patient identifiable” data extract, and for either a secondary purpose⁴ or for direct patient care, drawing on advice from the Department of Health Information Governance Policy Team, the National Information Governance Group, the NHS Information Centre and/or other bodies as appropriate; and
- c) approved by the Independent Advisory Group ensuring through a risk and benefit analysis that the extraction is, in the view of the Independent Advisory Group, appropriate and in the public interest; and
- d) authorised by the practice, who will be given fair and sufficient information and reasonable time and choices (see section on “*General Practice Participation*”) on whether to participate in queries; and
- e) publicised through a public website (as well as general information about GPES being made available through practices).

³ 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 http://www.dh.gov.uk/en/Managingyourorganisation/Informationpolicy/PatientConfidentialityAndCaldicottGuardians/DH_4100550.

⁴ 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 will be introduced to capture a patient’s preference to be excluded from disclosures by general practices for secondary uses.

All data extracted from a practice by GPES will be:

- a) Stored, processed and transmitted securely; and
- b) accessible only through role-based access controls⁵ (and with all accesses recorded in audit trails)⁶ to:
 - i. the general practices providing the data,
 - ii. authorised GPES users⁷ (contractor and NHS IC personnel), and only where necessary to ensure the data are processed correctly, **and**
- c) released to customers when processing is complete, but only where customers have signed a data sharing agreement with the NHS Information Centre stipulating that the data will be stored securely and accessed and used only for agreed purposes and in line with non-disclosure policies⁸; **and**
- d) deleted from GPES data stores as soon as the data have been released to, and accepted by, customers.

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

Although data will be held for only a short period of time, GPES will respond to any requests from patients asking for a copy of the information held about them⁹. Patients are also entitled to ask GPES customers to provide a copy of information held about them.

Practices will be asked to take steps to inform patients about GPES, the types of information extracted from GPES, and about the opportunities for patients to prevent disclosure of confidential information, at least two months before GPES implementation begins.

Where GPES is notified that it has received inaccurate personal data¹⁰, GPES will inform the source of the data (the 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.

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.

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

Controls applicable to different types of GPES queries

Note that where the only data recipient for the query is the practice itself¹¹, none of the controls in this section applies.

Where all the data extracted from a practice through GPES are “effectively anonymised at the time of extraction, or wholly inaccessible by any user until they have been effectively anonymised¹², then:

- a) Data covering all patients could be included in queries¹³; **and**
- 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 use and reuse agreements with the NHS Information Centre.

Where patient identifiable data extracted from a practice are potentially accessible by authorised GPES users 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 choices¹⁴, where adopted by general practice systems, will be respected, so that no restricted information will be extracted; **and**
- b) Patient consent, Section 251 approval¹⁵, or statutory justification¹⁶ will be required; **and**

¹¹ Some national customers are considering making requests for GPES to extract practice information solely for use by the practice.

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 opt outs 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* page 33).

¹⁴ The relevant choices with respect to 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> and page 10 of www.connectingforhealth.nhs.uk/systemsandservices/demographics/docs/comms/pdsguide.pdf

¹⁵ Section 251 approval is a possible alternative to consent where gaining patient consent is not practicable. See: <http://www.nigb.nhs.uk/ecc/about-the-ecc>. 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.

¹⁶ One example is *Confidentiality and Disclosure of Information: General Medical Services, Personal Medical Services and Alternative Provider Medical Services Directions 2005* and the associated Code of Practice which require the provision of patient identifiable data to PCTs without consent in certain circumstances and which permit it in other circumstances where it is not feasible to anonymise the data or gain patient consent (see in particular paragraphs 15 and 30-32 of the Code of Practice at http://www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicyAndGuidance/DH_4107303). However, there are no plans for GPES to be used in such circumstances; PCTs should approach practices directly where they wish to use the powers in these Directions to obtain patient identifiable data without consent.

- c) Where data are extracted for secondary purposes (see section on “*General Principles*”), no patient data will be extracted if the practice has recorded a patient’s request to be excluded from disclosures for secondary uses even where Section 251 approval has been given (but patient data will be extracted where the disclosure is for direct patient care¹⁷, or required by law); **and**
- 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 use and reuse agreements with the NHS Information Centre.

Where data extracted from a 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; **and**
- b) Patient consent, Section 251 approval, or statutory justification will be required; **and**
- c) Where data are extracted for secondary purposes (see section on “*General Principles*”), no patient data will be extracted if the practice has recorded a patient’s request to be excluded from disclosures for secondary uses even where Section 251 approval has been given (but patient data will be extracted where the disclosure is for direct patient care, or required by law); **and**
- d) Customers may disclose these data to other parties:
 - i. for “medical purposes”¹⁸ and where agreed by the Independent Advisory Group and other approval bodies, or
 - ii. where disclosure is required by law (e.g. in response to a court order).

Aggregated data extracted for the purpose of paying practices (such as QOF data) will be considered effectively anonymised so that payments made are accurate.

¹⁷ 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.

¹⁸ 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.

General Practice Participation

A practice will be able to change any of its choices at any time. When a query is run, current preferences will be used.

This includes an opportunity for practices to view data extracted and opt out of a query before the data are sent to the customer.

Participation in GPES

There will be one general choice, supported by a data processing agreement between GPES and the practice: the practice will be asked to choose whether or not practice data may, in general, be extracted for queries outputting "effectively anonymised" data.

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.

Where no response is received from a practice about the general choice above, or about a particular query, GPES will assume "no"¹⁹ and will not extract data.

GPES will always respect practice choices about access to practice data²⁰. It is expected that all practices will agree to certain essential extracts such as QOF (which is a planned GPES query). General Medical Services contractors are required to provide Primary Care Trusts with "any information which is reasonably required by the Primary Care Trust for the purposes of or in connection with the contract" and "any other information which is reasonably required in connection with the Primary Care Trust's functions"²¹ (subject to the considerations outlined in footnote 15).

Opt in or out of specific queries

Regardless of their general preference with respect to effectively anonymised queries (see the section '*Participation in GPES*' above), a practice may choose a different preference with respect to a particular query²². So, even if a practice has chosen "yes" in relation to effectively anonymised queries, they may choose "no" in relation to a particular query.

Before every patient identifiable query is run, practices will be asked to agree to the extract.

¹⁹ Without explicit practice agreement, access may be unauthorised and not consistent with the Data Protection Act.

²⁰ 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.

²¹ See Paragraph 77 of Schedule 6 to the *NHS (General Medical Services Contracts) Regulations 2004* at: <http://www.opsi.gov.uk/si/si2004/20040291.htm>

²² A GPES query is software which extracts data which may be run one or more times (each one a "query instance").

Notification of queries

Practices will be notified about all GPES queries before they are run. The only exception to this is that practices whose general choice is to allow effectively anonymised queries can subsequently choose to not be notified about each of those queries,

The 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 practice, GPES will assume b) – before every instance of the query being run.

Practices will be able to change their notification preferences at any time. Details of all queries will be published before they are run (after consideration by the Independent Advisory Group). Practices will be able to view, and if necessary revoke, practice data being output before it is sent to the customer.

GPES will always follow a practice notification preference unless the Independent Advisory Group decides that all practices should be notified of a query regardless of their preferences. This might happen where the Independent Advisory Group feels there is a particularly strong public interest in running a certain query (e.g. to identify health needs during a pandemic).

Document control

Reviewers

Version	Reviewers	Role
0.1	Karen Thomson	Information Governance lead, National Information Governance Board
0.1 - 0.5	Dave Roberts	GPES Project Director
0.2	Joan Higgins, Karen Thomson, Hilary Newiss, Stephen Hinde	NIGB GPES reference group members
0.3, 0.5	Matt King, Stuart Bloom, Alan Payne, Lizzie Whewell, Miles Garside, Paul Lucas, Alistair Lord, Tony Smith, Terence Shird	GPES project team members
0.3, 0.5	Clare Sanderson	NHS IC IG Director
0.5	Dawn Foster	NHS IC Information Governance
0.5	Simon Child, John Lockley, Ralph Sullivan, Neill Jones, Joanne Bailey	GPES GP Consultation Group
0.5	Hugh Stewart	Medical Defence Union
0.5	Grant Ingrams	British Medical Association
0.5	Philip Leech, John Wardell, Jill Matthews, Julian Flowers	GPES Project Assurance Group
0.5	Nick Clements	Medical Protection Society
0.5	Phil Walker, Paul Eveson	Digital Information Policy, Department of Health
0.5	Jane O'Brien, Michael Keegan	General Medical Council
0.5	Ade Adeagbo, Marlene Winfield, Vanessa Bourne, David Rabjohns, Fleur Fisher, Rod Mitchell	GPES Patient Consultation Group
0.6, 0.7	Catherine Jenkins, Steve Rowlands, Phil Walker	Department of Health
0.6	Geraldine Taggart-Jeewa	GPES Practice Manager Consultation Group
0.6	Neill Jones, Ralph Sullivan, Simon Child	GPES GP Consultation Group

Published by The NHS Information Centre for health and social care

This publication may be requested in large print or other formats.

Responsible author

General Practice Extraction Service (GPES) – Malcolm Oswald

For further information:

www.ic.nhs.uk

0845 300 6016

enquiries@ic.nhs.uk

Copyright © 2010 The Health and Social Care Information Centre, General Practice Extraction Service (GPES)

All rights reserved.

This work remains the sole and exclusive property of the Health and Social Care Information Centre and may only be reproduced where there is explicit reference to the ownership of the Health and Social Care Information Centre.

This work may be re-used by NHS and government organisations without permission.

This work is subject to the Re-Use of Public Sector Information Regulations and permission for commercial use must be obtained from the copyright holder.