Data Controller Agreement

Between NHS England and HSCIC
for the primary- secondary care linked dataset

[Insert date effective from]

[Insert version no.]

<DOCUMENT CONTROL>

(NB This section will be removed and/or replaced by Gateway reader box information upon publication)

Reviewers:

This document must be reviewed by the following:

Name	Signature	Title / Responsibility	Date	Version
Karen Thomson		Head of Strategic Information Governance NHS England	15/12/2014	
Rachel Merrett		Deputy Head of Strategic Intelligence NHS England	27/11/2014	
Dawn Foster		Head of Information Governance - HSCIC	22/10/2014	
Trevor Anders		Programme Manager Care.data Programme HSCIC	28/11/2014	

Approvals:

This document must be approved by the following:

Name	Signature	Title / Responsibility	Date	Version
David Roberts		IAO – Care.data programme HSCIC	28/11/2014	
Ronan O'Connor		Interim Director of Intelligence and Strategy NHS England	06/01/2015	
Geraint Lewis		IAO - NHS England	06/01/2015	
Eve Roodhouse		Care.data programme director - HSCIC	06/01/2015	
HSCIC Board				

Amendment History:

Version	Date	Amendment History
0.01	28/11/2014	Draft for review
0.02	17/12/2014	Accepted tracked changes from TA & DR
0.03	19/12/2014	Addition to 6th principle requested by Ronan O'Connor
0.04	05/01/2015	VB amendments following comments from Eve Roodhouse
0.05	06/01/2015	RM amendments following comments from Eve Roodhouse

	Data controller Agreement
1.	**Between**: NHS England and the Health and Social Care Information Centre (HSCIC)

Please note that NHS England is the operating name for the NHS Commissioning Board, which was established under Section 9 of the Health and Social Care Act 2012. This document hereafter refers throughout to NHS England.

2. Definitions

In this Agreement the following words have the following meanings:

Confidential patient information	Patient information is "confidential patient information" where— (a) the identity of the individual in question is ascertainable— (i) from that information, or (ii) from that information and other information which is in the possession of, or is likely to come into the possession of, the person processing that information, and (b) that information was obtained or generated by a person who, in the circumstances, owed an obligation of confidence to that individual.
Customer	A GPES customer is an organisation that has been sponsored by the Department of Health and NHS England and has submitted a request/query for data. Each customer request must be reviewed by the HSCIC and this includes review by the GPES Independent Advisory Group.
Data Protection Act	means the Data Protection Act 1998 and any subsidiary or subordinate legislation as the same may be varied or replaced from time to time
Data	Data means information which – (a) is being processed by means of equipment operating automatically in response to instructions given for that purpose, (b) is recorded with the intention that it should be processed by means of such equipment, (c) is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system, (d) does not fall within paragraph (a), (b) or (c) but forms part of an accessible record as defined by section 68 of the DPA, or (e) is recorded information held by a public authority and does not fall within any of paragraphs (a) to (d).
Data controller	as defined in the Data Protection Act 1998 – means a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are to be processed
General Practice Extraction Service (GPES)	The General Practice Extraction Service is a centrally managed data extraction service that will be used to obtain information from the majority of NHS general practice clinical systems in England with the aim of improving patient care.
"Joint" Data Controller	"Joint" covers the situation where the determination is exercised by data controllers acting together, typically with written agreements setting out the purposes for processing, the manner of processing and the means by which joint data controller responsibilities will be satisfied. All must have the authority to determine or prevent data processing, i.e. that they are consulted is insufficient to qualify them as a data controller. This is opposed to data controllers "in common", where data controllers share a pool of personal data, each processing independently of the other.
Hospital Episode Statistics (HES)	HES is a data warehouse containing details of all admissions, outpatient appointments and A&E attendances at NHS hospitals in England.
Pathfinder	Pathfinder Clinical Commissioning Groups and their member practices are working with NHS England and the HSCIC to help

	test, evaluate, influence and shape the extraction of GP data, and all supporting activity, within the care.data programme. There are 6 CCG pathfinders in 4 areas of England: • Blackburn with Darwen CCG • Leeds North CCG • Leeds South and East CCG • Leeds West CCG • North Hampshire CCG • Somerset CCG
Personal data	Personal data means data which relate to a living individual who can be identified – (a) from those data, or (b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.
Primary - secondary care linked dataset	For the purpose of this document primary care data refers to the data collected from GP practice clinical systems and secondary care data refers to Hospital Episode Statistics (HES).
Processing	Processing, in relation to information or data, means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data (which includes, in relation to personal data, obtaining or recording the information to be contained in the data), including – (a) organisation, adaptation or alteration of the information or data, (b) retrieval, consultation or use of the information or data, (c) disclosure of the information or data by transmission, dissemination or otherwise making available, or (d) alignment, combination, blocking, erasure or destruction of the information or data
Sensitive personal data	means personal data consisting of information as to: - (a) the racial or ethnic origin of the data subject (b) his/her political opinions (c) his/her religious beliefs or other beliefs of a similar nature (d) whether he/she is a member of a trade union (e) his/her physical or mental health or condition (f) his/her sexual life (g) the commission or alleged commission by him/her of any offence, or (h) any proceedings for any offence committed or alleged to have been committed by him/her, the disposal of such proceedings or the sentence of any court in such proceedings

3. **Purpose, objectives and legal basis**:

The Health and Social Care Act 2012 (H & SC Act 2012) creates a statutory obligation for health service bodies including GP practices to disclose information to the Health and Social Care Information Centre (HSCIC) in certain circumstances, for example to comply with a direction for information from NHS England.

GP practices have dual responsibilities. Under the Data Protection Act there is a statutory obligation to process personal data fairly and under the Health and Social Care Act there is a statutory obligation to disclose the data.

The HSCIC and NHS England are joint data controllers for the primary - secondary care linked dataset as part of the pathfinder stage of care.data programme once the data have been disclosed to the HSCIC. As data controllers, the HSCIC and NHS England are both obliged to comply with the Data Protection Act and other legal requirements such as the common law duty of confidence where it continues to apply within the context of the provisions of the H & SC Act 2012.

NHS England and the HSCIC are considered to be joint data controllers, in essence, because NHS England is responsible for determining the purpose for the collection and the HSCIC will determine the manner of the processing. The HSCIC can only disseminate confidential patient information where permitted by law and as set out in the H & SC Act 2012.

The purpose of this document is to set out the allocation of data controller responsibilities between the two organisations i.e. which organisation, is in practice, responsible for which elements of compliance and where joint decision-making processes are needed and to outline the mechanisms in place to resolve issues.

4. ***This section sets out the responsibilities that must be undertaken by the organisations party to this Agreement. Each requirement relates to the 8 Data Protection principles specified within the Data Protection Act 1998.***

1st principle

Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless:-

(a) at least one of the conditions in schedule 2 is met, and

(b) in the case of sensitive personal data, at least one of the conditions in schedule 3 is also met

Responsible organisation(s)	Joint NHS England and HSCIC
Planned compliance	In order for personal data to be processed lawfully, there is a need to consider other legal requirements such as the provisions of the H & SC Act 2012, and the common law duty of confidentiality where applicable in relation to dissemination by the HSCIC in light of Sections 261 & 262. In order for processing to be fair, patients, and those people legally empowered to act on their behalf, must be informed about how identifiable data about them are used. Whilst the fair processing obligation rests with the GPs, NHS England and the HSCIC are undertaking awareness raising activities to inform patients about how the national collection and linkage of primary care data as part of the care.data programme might affect the privacy of personal data. GP practices are data controllers and must provide fair processing information to patients, to the extent of informing them that the data is to be used for other purposes other than that which it was collected. This means that GP practices should take reasonable steps, so far as is practicable, to ensure that patients are made aware of, and understand: • the requirement, for data from their medical records to be provided to the HSCIC • how and when their GP practice will disclose it • that they can opt out and how they may do so • where to find out more information about why the information is being extracted what it will be used for and how it will be processed by HSCIC

	GP practices should actively provide the information described above to all registered patients including those who do not regularly visit the surgery. The care.data programme will provide materials and advice to support GP practices. The HSCIC and NHS England also have fair processing responsibilities. The HSCIC and NHS England must produce the detailed fair processing information necessary and sufficient to enable patients to opt out and have their questions answered. Under the Health and Social Care Act 2012, the HSCIC is empowered to require general practices to supply information about patients, if directed to do so by NHS England. Patient consent is not legally required for disclosure. Under the Act, NHS England may stipulate whatever data it considers "necessary or expedient"[1], although it must seek advice first from the HSCIC. NHS England has made clear what data it considers to be necessary. (The link to the data items is documented in page 5 under the 3rd DPA principle.) Under the Data Protection Act (Schedules 2 and 3), the condition for processing the personal data is that the processing is necessary because of a legal obligation (paragraph 3). Sensitive personal data are being extracted, and the relevant condition for this under Schedule 3 of the Act is that the processing is necessary for medical purposes (paragraph 8), which includes health service management and medical research. The Government has made a commitment that patients have a right to object to the use of their confidential patient information for purposes beyond their direct care. The Secretary of State for health will direct that confidential patient information should be extracted from GP electronic medical records unless the patient has objected. The patient's objection is recorded as a code on their medical record at the GP practice.
2nd principle **Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes**	
Responsible organisation(s)	Joint NHS England and HSCIC
Planned compliance	The care.data programme aims to increase the range and detail of information that is collected across all NHS-funded services for purposes beyond direct care. The plan is to securely connect information together and make it available to those who plan NHS services, researchers, medical charities and businesses that support the NHS to make services better. The first phase of the care.data programme is to collect and securely connect information into a primary – secondary care linked dataset.
3rd principle **Personal data shall be adequate, relevant and not excessive in relation to the purpose or**	

[1] In the case of personal or confidential data obtained without consent then the test is one of necessity rather than expedience to align with the requirements of the DPA and the HRA

purposes for which they are processed	
Responsible organisation(s)	Joint NHS England and HSCIC
Planned compliance	Only the agreed data sets will be used. GP representatives and an independent advisory group have been involved in deciding which health, care and treatment information should be extracted. The proposed extract is based on four groups of data: demographics, events, referrals and prescriptions. Alongside this, there is a set of selection criteria for specific conditions or disease types. Coded information that has been recorded in the patient's medical record will be extracted, such as vaccinations, biological values (such as blood pressure, BMI and cholesterol with Quality and Outcomes Framework (QOF) exceptions codes), referrals, prescriptions and diagnoses. These diagnoses relate to health conditions such as diabetes, heart disease, stroke, cancers (including bowel, breast, and cervical), chronic liver disease, chronic kidney disease, asthma, high blood pressure and dementia. Written notes such as details of conversations a GP has had with their patients will not be collected. The data items are listed within the primary care technical specification: http://www.england.nhs.uk/wp-content/uploads/2013/05/ces-tech-spec-gp-extract.pdf The secondary care data set, to which the primary care data will be linked, is defined here: http://www.hscic.gov.uk/hes The linkage of the data requires sufficient identifiers to validate patient identity for linkage purposes and therefore:-The patient's date of birth, postcode, NHS number, and gender (but not name or full address) will be used to link their records in a secure environment at the HSCIC but will then be removed. Once this information has been linked, a new record and reference number will be created that does not identify the patient either from the content of the record or the reference number.
4th principle **Personal data shall be accurate and, where necessary, kept up to date**	
Responsible organisation(s)	HSCIC
Planned compliance	The required data will only be extracted from general practice clinical computer systems (i.e. from patients' electronic health records). There will be no extraction of data from any other electronic system within the practice, irrespective of whether the system is maintained by the general practice. If any data errors or omissions are present within these systems, there will be corresponding errors and omissions in the data provided to the customer. Consequently, there is no assurance that the returned data meets the key data quality principles of: • Accuracy – that the data has been accurately captured. For instance, that a BMI score of 22.4 has been inadvertently recorded in the general practice system as 12.4.

	• Completeness – that the system captures each diagnosis, symptom, intervention and activity related to each patient. There may be cases where patients do not access general practice services for each health related problem or because general practices only capture primary symptoms and diagnoses. It is therefore possible that the data may be under reported. • Timeliness – that the data contains all diagnoses, symptoms, interventions and activities to the reporting period end date. There may be cases where there is a time lag between an event occurring and data for that event being recorded in the general practice system. The HSCIC intend to develop a set of data quality indicators based on the extracted data and use this to inform potential customers of any data issues/factors they should take into consideration when analysing the data. These data quality indicators will be used to provide a report back to GP practices regarding the quality of their data. HSCIC will be responsible for linking the extracted data. The NHS number, postcode, date of birth and gender will be extracted by the HSCIC to ensure that records are correctly and accurately linked together. The HSCIC will provide a measure of the quality of the linkage.
5th principle **Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes**	
Responsible organisation(s)	NHS England and HSCIC to agree rules jointly. HSCIC solely responsible for day-to-day application of rules.
Planned compliance	The original extract of data from a GP practice will be held long enough to enable processing and linkage, and will then be permanently physically erased. The linked data will be retained in the Health and Social Care Information Centre. Access to the data by organisations outside of the HSCIC will be controlled through the HSCIC Data Access Request Service (DARS) (www.hscic.gov.uk/dars) process. As part of the DARS process the organisation must agree to terms and conditions in a Data Sharing Contract (DSC) and Data Sharing Agreement (DSA). The contract and agreement include terms and conditions requiring the organisation to permanently destroy/delete or erase the data, together with all hard or soft copies of the same on expiration of the DSA or termination of the DSC or earlier if use of the data is completed. After an organisation receives data, an HSCIC audit function will monitor adherence to the DSC and DSA and will stop the flow of data if the HSCIC has any concerns about the organisation Most research is based on longitudinal studies going back over several decades of data in order to build up a comprehensive picture and ensure accurate conclusions can be drawn from the data. As these data are intended for use in such long-term studies in the future it is expected the data would be retained for a minimum of 25 years. However the retention of the linked data will be reviewed after a period of 10 years, to consider if retention is no longer necessary, or to identify a further retention and review period as necessary.

6th principle **Personal data shall be processed in accordance with the rights of data subjects under the DPA**	
Responsible organisation(s)	HSCIC
Planned compliance	HSCIC will be responsible for making decisions on applications for access and distribution to the data including the: • lawfulness of the application including considering the type of data being requested and the purpose for which the data is being requested; • administration of subject access requests directed to the HSCIC; • administration of Freedom of Information requests directed to the HSCIC; • administration of Parliamentary Questions directed to the HSCIC; • consideration and application of objection codes in line with guidance from the Department of Health and NHS England; • administration of any other requests under any other legal/statutory purposes set out under UK and/or European Union legislation • lawfulness of disclosures to other parties in line with directions relating to dissemination. Where such an application is approved the HSCIC will be responsible for determining the media/method for providing the data, the content and the range of the data that should be provided. The HSCIC will publish on its web pages the details of the data it holds in relation to this dataset and the purposes for which that data can be used and information regards how a patient can object to the use of their data in this way including how they can request the prevention of the use of their data in identifiable form The HSCIC will share communications and agree handling with NHS England ahead of publication of details in relation to this dataset.
7th principle **Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data**	
Responsible organisation(s)	HSCIC responsible for compliance with NHS England seeking and receiving assurance of compliance
Planned compliance	The data will flow securely, to the HSCIC, which will process, link and store the data ensuring that patient confidentiality is protected. It is intended that the General Practice Extraction service will be used as the principal route through which the data will be extracted and sent to the HSCIC. However GP practices will be given the option of agreeing an alternative mechanism to extract and flow the data to the HSCIC but it must be acceptable to the HSCIC. The HSCIC has a process for reporting suspected data breaches.

All of the HSCIC's systems and services are designed and operated in accordance with multiple international security standards and best practices. This means that information in IT systems is protected, staff are trained in information governance responsibilities, information is managed securely, and the organisation processes sensitive information ensuring full compliance with the law.

There is substantial protection around the technical infrastructure for the primary-secondary care linked dataset. The HSCIC manages the secure infrastructure that is used to transfer data from practices.

The transfer of data between GP systems and GPES uses the Digital Transfer Service (DTS) mailbox solution, which encrypts a file exported from the GP system and then securely transfers this to the HSCIC's DTS datastore.

The HSCIC holds data in accordance with the highest industry standards (specifically ISO27001/2 – Information Security Standard). This holds the following features:

a. data processing does not take place outside of the UK;
b. access is strictly controlled and limited to those who need it for their role;
c. secure networks used to transfer data are regularly tested and monitored for any vulnerabilities (hacking and other types of attack); and
d. audits and spot checks are made to make sure that standards are being maintained and any deficiencies are dealt with promptly.

There is a strict accreditation process that is applied to members of staff within the HSCIC who handle data, which also includes specific training according to role. Query history is retained centrally and can be audited upon request.

During the pathfinder stage access to the primary – secondary care linked dataset, by organisations other than Pathfinder CCGs accessing their own data, will only be available through a Secure Data Facility at the HSCIC.

This Secure Data Facility is a physical environment through which authorised and audited access to sensitive data can be granted, and is secured through the application of defined technical controls and documented processes in order to meet regulatory requirements.

The primary objective of such a facility is to ensure the security of particularly sensitive data, with access restricted to approved users only, from an authorised location. This ensures access is granted for a specific purpose, and user actions are recorded and clearly auditable, thereby ensuring transparency and traceability is maintained.

8th principle
Personal data shall not be transferred to a country or territory outside the European

Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data	
Responsible organisation(s)	HSCIC
Planned compliance	HSCIC stores and processes the data within the UK. Any recipients of data from the HSCIC must declare where data are to be processed and must have in place appropriate policies and procedures and be able to demonstrate safeguards. The Health and Social Care Information Centre (HSCIC) is accountable for the security of personal information. Information is managed appropriately, and the organisation disseminates sensitive information ensuring full compliance with the law. All applications for access to data consider the proposed security measures and where the data are to be processed and stored to ensure compliance with this principle. Data sharing contracts and data sharing agreements are put in place with all organisations that are approved to receive/access the data to contractually reinforce the agreements as to where the data will be processed, stored and disseminated as stated in the application. During the pathfinder stage access to the primary care – secondary care linked dataset, by organisations other than Pathfinder CCGs accessing their own data, will only be available through a Secure Data Facility at the HSCIC.
Additional requirements requiring explicitly documented arrangements	
Compliance with: **a) Information Commissioner's Office (ICO) Data Sharing Code of Practice** **b) Anonymisation Standard for Publishing Health and Social Care Data – ISB 1523** **c) ICO Anonymisation: managing data protection risk code of practice**	
Planned compliance	The Care Act 2014, introduced a new clause that places additional restrictions on dissemination of information by the HSCIC. The new clause amends sections 253, 261 and 262 of the Health and Social Care Act 2012 to insert a general duty for the HSCIC "to respect and promote the privacy of recipients of health services and of adult social care in England". Apart from in limited circumstances where there is a statutory requirement to disclose data, the new clause ensures that the HSCIC can only disseminate information to requesting organisations if "disseminating the information would be for the purposes of the provision of health care or adult social care, or the promotion of health." It also requires the HSCIC "to have regard to any advice given to it by a committee appointed by the Health Research Authority". Section 60 of the Health and Social Care Act 2001 as re-enacted by Section 251 of the NHS Act 2006 allows the Secretary of State for Health to make regulations to set aside the common law duty of confidentiality for defined medical purposes. The HRA took on responsibility for Section 251 in April 2013, establishing the Confidentiality Advisory Group (CAG) function. The information released by the HSCIC will not identify individuals unless there

		is a legal basis e.g. Court Order or statutory requirement. The HSCIC will judge that no excessive data will be released to customers and will ensure that any data released is covered by appropriate terms and conditions with customers. In accordance with the recommendation of the GPES Independent Advisory Group during the pathfinder stage no applications for personal confidential data will be considered where the applicant has received Section 251 approval. The application and approvals processes for HSCIC data are available on the Data Access Request Service web page at www.hscic.gov.uk/dars Before any organisation can receive/access the data, they must agree to terms and conditions in a data sharing contract, which includes penalties for misuse. These conditions include: • That use of the information is limited to specific purposes relating to the provision of health care or adult social care, or the promotion of health. • That the data cannot be disclosed further. • Security requirements for the organisation receiving the data. Each customer will sign a data sharing agreement, which sets out the rules and conditions under which the data can be used and shared. After an organisation receives data, an HSCIC audit function will monitor adherence to data sharing contracts and will stop the flow of data if the HSCIC has any concerns about the organisation. The HSCIC is committed to transparency and being open with citizens about who has access to their data and why. A Register began publishing in April 2014 and is being updated quarterly. It lists each organisation, the type of data released, the legal basis for release and the purpose for which the data was provided. The register is intended to encourage public scrutiny of HSCIC decisions. The register is available via the HSCIC website at: www.hscic.gov.uk/dataregister.
5.	**Commencement of Agreement** ***Specify the date the Agreement will come into force*** ***(TBC)***	
6.	**Length of Agreement** ***How long will the agreement remain in force*** ***(TBC)***	
7.	**Review of Agreement** ***Specify when the agreement will be reviewed*** This agreement should be reviewed at the end of the pathfinder stage.	
8.	**Dispute Resolution** Any disputes arising between the parties will be resolved initially between the Information Asset Owners of NHS England and the HSCIC. If resolution cannot be reached the issue should be escalated to Tim Kelsey, National Director of Patients & Information and Carl Vincent, Interim Director of Information and Analytics and then to the Chief Executive of the respective	

	organisations.
9.	**Persons responsible for the development and review of this Agreement** *Specify Job Title and Organisation to enable relevant parties to be part of the review* Jenny Spiers, Information Governance Specialist – Transition Programme NHS England Karen Thomson, Head of Strategic Information Governance, Intelligence & Strategy, NHS England Rachel Merrett, Deputy Head of Strategic Intelligence, NHS England Trevor Anders, Programme Manager, Care.data Programme, HSCIC Dawn Foster, Head of Information Governance, HSCIC Ronan O'Connor, Director of Intelligence, NHS England

Data Controller Agreement
for the primary- secondary care linked dataset
Signatures

Signed for and on behalf of : NHS England	
Name:	
Position:	
Signature:	
Date:	

Signed for and on behalf of :

The Health and Social Care Information Centre (HSCIC)

Name:	
Position:	
Signature:	
Date:	