NHS
Cambridgeshire and Peterborough
Clinical Commissioning Group

Cambridgeshire and Peterborough Clinical Commissioning Group (CCG)

Controlled Environment for Finance (CEfF) Policy 2021-2023

Ratification Process

Lead Author:	Corporate Services Manager (IG Lead)
Developed by:	Information Governance Team
Approved by:	Information Governance, Business Intelligence & IM&T Steering Group 15th July 2021
Endorsed by:	Integrated Performance and Assurance Committee 24th August 2021
Ratified by:	CCG Governing Body – 7th September 2021
Version:	4.0
Latest Revision date:	July 2023 (or earlier if significant change to local or national requirements)
Valid on:	7th September 2021

Document Control Sheet

Development and Consultation:	Policy developed in consultation with the IG, BI & IM&T Steering Group and Information Governance, Business Intelligence and Finance teams and endorsed by Clinical Executive Committee July 2015.
Dissemination	This Policy is relevant to all staff working for the CCG who are involved in the creation, submission, receipt, validation, or payment of invoices for health care services funded by the NHS. The Policy will be available on the CCG website; Staff will be advised of the Policy via the weekly Staff Comms.
Implementation	Policy implementation involves all staff and managers and will be monitored by the IG, BI & IM&T Steering Group.
Training	Role specific training will be provided to the staff members with direct access to the CEfF information.
Audit	Implementation of the Policy will be monitored on a regular basis and the associated standard operating procedure for the process audited annually.
Review	The document will be reviewed in July 2023 or earlier dependent on local or national changes.
Links with other policies and procedures	The Policy should be read in conjunction with: Who Pays? Determining responsibility for payments to providers August 2013; Who Pays? Information Governance Advice for Invoice Validation; CCG CEfF Compliance Statement; Staff/User Training – Invoice Validation in Integrated Single finance System (ISFE); CCG's Privacy and Fair Processing Notice.
Equality and Diversity	The OD & HR Advisor (Equality & Diversity) carried out an Equality & Diversity Impact assessment and concluded the policy is compliant with the CCG Equality and Diversity Policy. No negative impacts were found.

Revisions

Version	Page/ Para No	Description of change	Date approved
0.1		Creation	
1.0		Ratified by CMET	July 2015
2.0	Whole document review	Revised in accordance with NHSE's update on processing of personal data for invoice validation March 2017	July 2017
3.0	Whole document review	Revised to reflect approval of NHSE's application for extension of s251 support until September 2020 and inclusion of NHSE's role specific training requirement for staff members whose roles require use of the Integrated Single Finance System (ISFE).	27th August 2019
4.0	Whole document review	Biennial Review. Introduction updated to reflect that the Confidentiality Advisory Group (CAG) gave their approval to extend s251 support for Invoice Validation data processing (CAG 7-07(a-c)/2013) to the end of September 2022.	15th July 2021 IG, BI and IM&T Steering Group

Table of Contents

1. INTRODUCTION

Cambridgeshire and Peterborough Clinical Commissioning Group (CCG) recognises the need for an appropriate balance between openness and confidentiality in the management and use of information. The CCG fully supports the principles of corporate governance and recognises its public accountability, but equally places importance on the confidentiality of and the security arrangements to safeguard both personal information about patients and staff and commercially sensitive information. The CCG also recognises the need to share information with other health organisations and agencies in a controlled manner consistent with legislative requirements.

Invoice validation is part of the process by which providers of care or services get paid for the work they do. Invoices are submitted to the commissioners of their service for payment, but before payment can be released, commissioners need to ensure that the activity claimed for each patient is their responsibility.

The introduction of the Health and Social Care Act 2012 changed the structure of the NHS. This Act, which became law on 1 April 2013, did not provide a clear legal basis for clinical commissioning groups (CCGs) and commissioning support units (CSUs) to set aside the common law duty of confidentiality for this purpose.

On 22 November 2013, the Secretary of State for Health approved applications from NHS England for Section 251 support for Personal Confidential Data (PCD) to be used to validate invoices lawfully, without the need to obtain explicit consent from the individual patient. Approval was subsequently extended to September 2020.

The Confidentiality Advisory Group (CAG) has now given their approval to extend s251 support for Invoice Validation data processing (CAG 7-07(a-c)/2013) to the end of **September 2022.**

2. PURPOSE AND SCOPE OF POLICY

The NHS England guidance 'Who pays? Determining responsibility for payments to providers' 2013, https://www.england.nhs.uk/wp-content/uploads/2014/05/who-pays.pdf helps CCGs to understand their commissioning responsibilities and to determine who pays for a patient's care.

Invoice validation is an essential procedure in the management of health and social care services. The process ensures that providers are reimbursed correctly for the care and treatment they have delivered to patients. It involves checking that the correct patient received the treatment as specified and that the right commissioner has been identified.

The invoice validation process supports the delivery of care by:

- Ensuring that service providers are paid for the patient's treatment;
- Enabling services to be planned, commissioned, managed and subjected to financial control;
- Enabling commissioners to confirm that they are paying appropriately for the
- treatment of patients for whom they are responsible;
- Fulfilling commissioners' duties for fiscal probity and scrutiny;

- Enabling invoices to be challenged and disputes or discrepancies to be resolved.

As CCGs do not have a legal right to access personal confidential data (PCD) they must ensure they have a secure legal basis for each purpose for which they wish to use such data.

The intention of this document is to provide the process by which the CCG implemented the section 251 approval and the use of 'necessary' PCD for invoice validation purposes.

The term 'necessary' means that it would not be reasonably feasible to achieve the intended purpose without using PCD.

Where the CCG is already validating invoices without the need to use PCD that practice is lawful and can continue without reference to the section 251 approval. Wherever possible the CCG will use anonymised or pseudonymised data to validate invoices and this principle applies to all invoice validation activity.

Currently the lawful basis to use PCD for invoice validation for individual, patient centred service (eg individual funding requests, personal health budget, continuing health care) is based on consent.

This procedure has been written to avoid the multiple transfers of data between different organisations and also within the CCG so as to create the minimum points of failure.

Although this policy is only directly applicable to staff working within the CEfF, it is still relevant to all staff working for the CCG who are involved in the creation, submission, receipt, validation, or payment of invoices for health care services funded by the NHS. This will include permanent, temporary and contract staff and will ensure that all staff are aware of the restrictions in use of PCD to support the invoice validation process. National guidance states that a maximum of three staff can sit within the CEfF environment. These had been nominated by the CCG.

3. DEFINITIONS (A-Z)

Accredited Safe Haven (ASH)
Established in either a CCG or Central Support Unit (CSU) as a controlled environment where staff can receive weakly pseudonymised data under section 251 approval (Reference CAG 2-03(a)/2013) and use the data for commissioning purposes, on the strict condition that staff do not have access to PCD or the means to identify an individual patient. Stage 1 ASH accreditation refers to those organisations that have completed the approval process.

Anonymisation
The process of removing identifiers from a set of data so that there is little, or no risk of an individual being identified from those data or by matching them to other data, ie identification is not likely to take place.

Backing Data
Activity information provided with a copy of the invoice to the CCG to evidence the health care services delivered and amount of payment claimed either under a commissioning contract or under a non-contract agreement. The backing data must follow the framework provided in Appendix 3.

Commissioning Data Set (CDS)
CDS forms the basis of data on activity carried out by organisations that is reported centrally for monitoring and payment purposes. These Data Sets supports the current version of the Healthcare Resource Group (HRG) used for the calculation of payment and monitoring of services.

Confidentiality Advisory Group
The Confidentiality Advisory Group (CAG) is an independent body which provides expert advice on the use of confidential patient information – including providing advice to the Health Research Authority (HRA). It also provides advice to the Secretary of State for Health for non-research uses. The key purpose of the CAG is to protect and promote the interests of patients and the public, while at the same time facilitating appropriate use of confidential patient information for purposes beyond direct patient care.

Consent
The approval or agreement for something to happen after consideration. For consent to be legally valid it must be unambiguous, involve a clear affirmative action (Opt in) and be given freely. The individual must be fully informed, understand the implications of their decision and have the capacity to make that decision.

The CCG must keep a record of consent if given. Consent cannot be taken from pre-ticked boxes or silence. Consent can be withdrawn at any time by the individual without reason. The right to withdraw consent and its implications should be communicated clearly to the individual when requesting consent.

Controlled Environment for Finance (CEfF)
The CEfF was a new concept established by the section 251 approval as a temporary measure to assist CCGs and CSUs manage the change process. Staff working in a CEfF will be able to see PCD under the terms of s251 applications. They are therefore subject to strict conditions to ensure accountability for keeping PCD secure. CEfFs will be aligned with a Stage 1 ASH.

Data Controller
Under Article 4 of the GDPR, a data controller is an individual or an organisation who determines the purposes for which any PCD are or will be processed and the manner of such processing. Data controllers must ensure that any processing of personal data for which they are responsible complies with the Data Protection Act 2018.

Data Processor
Under Article 4 of the GDPR, a data processor means any person (other than an employee of the data controller) who processes PCD on behalf of the data controller. Data processors are now directly subject to the Data Protection Act. The data subject will be directly subject to the GDPR if they go against the data controller's wishes and what is stated in their contract. The Information Commissioner recommends that organisations should choose data processors carefully and have in place effective means of monitoring, reviewing, and auditing of their processing. A

written contract detailing the information governance requirements must be in place to ensure their compliance with GDPR.

Data Services for Commissioners Regional Offices (DSCROs)
These are regional outposts of NHS Digital and operate under the statutory access powers of NHS Digital under the Health and Social Care Act 2012.

Health and Social Care Act 2012 (HSCA)
The HSCA amended the NHS Act 2006 and established CCGs as independent legal entities with responsibility for commissioning services for their local population and the NHS Commissioning Board ('NHS England') and NHS Digital.

Information Governance (IG)
How organisations manage the way information and data are handled within the health and social care system in England. It covers the collection, use, access and decommissioning of information as well as the requirements and standards that organisations and their suppliers need to achieve to fulfil the obligations that information be handled legally, securely, efficiently, effectively and in a manner that maintains public trust.

Integrated Single Finance environment (ISFE)
NHS England and NHS SBS have introduced a new mechanism within the Integrated Single Finance Environment (ISFE) system, which identifies suppliers, and their associated Commissioners (CCG), that submit Personal Confidential Data (PCD) for invoice validation purposes. The CCG is responsible for ensuring that the correct process is followed for the submission of PCD to validate invoices via the CCG's nominated Controlled Environment for Finance (CEfF).

Invoice
A bill for the provision of health care and treatment provided to a patient and submitted by the provider of those services to the CCG responsible for that patient.

Legal Bases
Consent is just one of the Legal Bases used for processing data. As consent can be withdrawn, it is advised that we look at all other legal basis before relying on that of consent. If you have a reason for processing data, such as for the purposes of provisioning healthcare, then it is advised that you use that as your legal basis. Individuals still have a say on how you process their data through an opt-out process highlighted in the CCG's Privacy and Fair Processing Notice.

Necessity
Many of the conditions for data processing depend on the processing being 'necessary' for a particular purpose to which the condition relates. This condition imposes a strict requirement because it will not be met if the organisation can achieve the purpose by some other reasonable means or if the processing is necessary only because the organisation has decided to operate its business in a particular way.

NHS Digital (formerly HSCIC)
The Health and Social Care Information Centre (HSCIC) now known as NHS Digital was set up as an Executive Non-Departmental Public Body (ENDPB) in April 2013. The functions and duties of the HSCIC are set out in Part 9 of the Health and Social Care Act 2012, in sections 252 to 275, and in Schedule 18.

NHS Shared Business Services (NHS SBS)
Please visit the NHS SBS website for further information:
https://www.sbs.nhs.uk/nhs-sbs-about-us

Payment by Results (PbR)
PbR is the payment system in England under which commissioners pay healthcare providers for each patient seen or treated, taking into account the complexity of the patient's healthcare needs. The two fundamental features of PbR are currencies and tariffs that are determined nationally. Currencies are the unit of healthcare for which a payment is made and can take a number of forms covering different time periods from an outpatient attendance or a stay in hospital, to a year of care for a long term condition. Tariffs are the set prices paid for each currency.

Personal Confidential Data (PCD)
This term describes personal information about identified or identifiable individuals, which should be kept private or secret. For the purposes of this policy, 'personal' includes the GDPR definition of personal data, but it is adapted to include deceased as well as living people. 'Confidential' includes both information 'given in confidence' and 'that which is owed a duty of confidence' and is adapted to include 'sensitive' (special category data) as defined in the Data Protection Act. Used interchangeably with 'confidential' in this policy.

Under Article 4 of the GDPR, personal data are Data that relate to a living individual who can be identified from that data and other information that is in the possession of or is likely to come into the possession of the data controller. It 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.

Privacy / Fair Processing Notice
Individuals should know and understand how their information is to used and shared, there should be no surprises. We do this by posting a Privacy / Fair Processing Notice on our public website. The Notice must clearly state how we process information, whether we share it and if so, who we share it with. The Notice must also inform individuals of how they can 'opt out' of their data being used. The CCG's Privacy / Fair Processing Notice can be accessed here

Processing
Under Article 4 of the GDPR, 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, including organisation, adaptation or alteration of the information or data; retrieval, consultation or use of the information or data; disclosure of the information or data by transmission, dissemination or otherwise making available; or alignment, combination, blocking, erasure or destruction of the information or data.

Pseudonymisation
Psudonymisation is the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

Data are considered to be anonymised where the recipient of the pseudonymised data set has no means of access to the algorithmic key to re-identify individuals. See also ‘weakly pesudonymised data’.

Public Interest (Test)
This test applies when the holder of the information believes that the public good that would be served by sharing the information outweighs both the obligation of confidentiality owed to the individual and the public good of protecting trust in a confidential service.

Section 251 (NHS Act 2006)
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 Regulations that enable this power are called the Health Service (Control of Patient Information) Regulations 2002. Regulation 5 provides the Secretary of State for Health with the power to set aside the common law duty requirement for consent to use personal confidential data for medical purposes other than the provision of direct healthcare and treatment, subject to advice from the Confidentiality Advisory Group. Any reference to section 251 support or approval’ actually refers to approval given under the authority of these Regulations.

Sensitive (Special Category) Data
Under Article 4 of the GDPR, these are data that identify a living individual consisting of information as to his or her: racial or ethnic origin, political opinions, religious beliefs or other beliefs of a similar nature, membership of a trade union, physical or mental health or condition, sexual life, convictions, legal proceedings against the individual, or allegations of offences committed by the individual. See also ‘Personal Confidential Data’.

Weakly Pseudonymised Data
Data that includes one strong item (eg date of birth or NHS number or postcode) that could be matched with other data and lead to the identification of an individual patient. The term is used in conjunction with a CCG accredited Stage 1 ASH. Outside the ASH, weakly pseudonymised data would be considered to be 'personal data' under the terms of the GDPR (Article 4). This concept aligns with the definition of de-identified data for limited access in the report of the Caldicott 2 Review of information governance.

4. RESPONSIBILITIES

Accountable Officer
The Accountable Officer has ultimate responsibility for compliance with IG legislations and guidance.

The Senior Information Risk Owner (SIRO)
The Senior Information Risk Owner is accountable for information risk on the Governing Body and in internal discussions. They will provide written advice to the Accountable Officer on the content of their Annual Governance Statement in regard to information risk.

The Caldicott Guardian
The Caldicott Guardian is a senior person with an advisory role within an organisation, they are responsible for (a) ensuring the confidentiality of patient and service-user information and (b) enabling appropriate information sharing.

The Information Governance Team
Responsible for ensuring that this policy is implemented, including any supporting guidance and training deemed necessary to support the implementation, and for monitoring and providing Governing Body assurance in this respect.

The Information Governance Lead is also responsible for advising on IG strategic direction, the development of policy and guidance for the CCG.

All staff working in the CEfF
All employees and anyone working on behalf of the CCG, involved in the receipt, handling or communication of person identifiable information for invoice validation purposes, must adhere to this policy to support the reputation of the CCG and where relevant of their profession. Everyone has a duty to respect a data subjects rights to confidentiality. A log of named access to demographics systems within the CEfF to validate invoices is kept ensuring that only three members of staff have access at any one time (See Appendix 1). Staff who are given access to patient data systems for the purpose of invoice validation sign the form at Appendix 2 as assurance of their compliance in completing their annual mandatory information governance training and have understand their responsibilities around confidentiality with regards accessing the systems.

5. LEGAL AND REGULATORY FRAMEWORK

The section 251 approvals are time-limited and are subject to conditions that the CCG and providers must follow in order to validate invoices legally.

The legal requirements, restrictions and exclusions that apply to the Section 251 support are set out in Regulation 7 of the Health Service (Control of Patient Information) Regulations 2002.

The specific and standard conditions for approval are listed in the Confidentiality Advisory Group's letter of 22nd November 2013.

NHS England and the HSCIC will define the application process, set out the standards expected, and provide detailed information about these conditions.

The CCG must comply with the law and best practice standards imposed by:
the section 251 regulations; other laws, such as the Data Protection Act 2018;
the Secretary of State for Health (as specified in the s251 approval letter);
professional bodies such as the General Medical Council.

The CCG must respect patient confidentiality in accordance with the NHS Constitution, NHS Digital's Guidance, and the Statutory Code of Practice. 'Necessity' is a qualifying condition to justify the lawful use of personal confidential data within:

- the GDPR and Data Protection Act 2018; and
- the Caldicott Principles.

6. OPERATION OF THE CEFF

The CEfF receives patient identifiable information which needs to be handled in a confidential manner. Therefore, the following must be used:

- A secure email address – CAPCCG.ceff@nhs.net;
- A secure (restricted) location within the CCG's Network;
- A specified and limited number of individuals with access to this information;
- In the case of Cambridgeshire and Peterborough CCG, we have been approved for three individuals with access to patient information for the purposes of the CEfF.

6.1 Receipt of data

6.1.1 The invoice is uploaded to Oracle by NHS SBS. Where possible, SBS will stop any invoices received by them that contain patient data.
6.1.2 The invoice comes into the workflow of the CCG.
6.1.3 The invoice is opened in Oracle by a member of the Finance team where it is checked, and cost coded. The invoice should contain contact details to obtain backing data if required.
6.1.4 If PID / PCD is found to be included anywhere on an invoice in the Non-PO workflow, users are able to return the invoice to NHS SBS for action by checking the 'Unable to Process' option and selecting one of the return options in Appendix 4.
6.1.5 The provider is advised that the invoice has been cancelled and that it should be resubmitted without containing PID.
6.1.6 The invoice is logged into a spreadsheet register.
6.1.7 Where required, backing data is requested via NHS mail – this is usually in the form of a spreadsheet containing GP and Postcode data. The Invoice is on hold at this point while this is being resolved.
6.1.8 The backing data is in the form of a spreadsheet containing GP and Postcode data along with NHS numbers/patient identifiers.
6.1.9 Backing data is saved to a secure folder within a restricted site with the Provider's name and deleted from the CEfF inbox.
6.1.10 Once the backing information has been received and reviewed against the invoice, the invoice is either accepted or challenged.
6.1.11 Where challenged, the invoice is returned to the provider.
6.1.12 Where accepted, the invoice is coded and checked on Oracle then submitted.
6.1.13 The invoice is forwarded to the Budget Holder for approval.

6.2 Retention periods

6.2.1 The backing information received into the CEfF email address should be deleted as soon as the information is saved into the designated Restricted folder.
6.2.2 Information contained within the Restricted folder is reviewed and securely deleted after 24 months to prevent double charging.
6.2.3 This will be a rolling year on resolved backing only, any unresolved data will be kept until resolved.

6.3 Cross-matching to determine responsible commissioner

6.3.1 The Data normally comes through with an invoice number on it or will state the month of the activity.
6.3.2 The CEfF Team will then match with the invoice once received.
6.3.3 The total of activity must match the amount of the invoice and description.
6.3.4 The CEfF Team then validates the data by ensuring that the NHS numbers belong to patients who were under C&PCCG at the time of the activity that the charges are correct.

6.4 How challenges will be responded to

6.4.1 An email will be sent from the CEfF email address to the secure email address which the data was originally sent.
6.4.2 This email will contain the data which is subject to challenge or query.
6.4.3 These email challenges will be moved from the 'sent box' in the CEfF to an appropriately named file on the restricted drive.

7. INDUCTION AND TRAINING PROCESSES

All employees who have access to the information provided via the CEfF will be required to have read the 'Who Pay's' Information Governance Advice.

7.1 Each member of the CEfF team is required to have read the confidentiality clauses in the general contract of employment.
7.2 Each member of the CEfF team is required to sign a proforma indicating that they have read and understood the 'Who Pay's' guidance and the confidentiality obligations imposed on them by contract.
7.3 Each member of the CEfF team will undertake mandatory Data Security Awareness Training annually, new members to the Team must complete the training on their first day in post and annually thereafter.
7.4 In addition to Data Security Awareness Training, CEfF Staff will refresh their knowledge using NHSE's Staff/User Training – Invoice Validation in Integrated Single finance System (ISFE) annually.
7.5 It is the responsibility of the Finance Manager to ensure that all CEfF staff have completed these requirements and have signed the proforma within Appendix 2 of this procedure.

8. AUDIT

8.1 Audit of the CEfF procedures will be undertaken by the Information Governance team.
8.2 The Audit frequency will be yearly or more frequently if required.

Annex A – Equality Impact Assessment Form

NHS
Cambridgeshire and Peterborough
Clinical Commissioning Group

Initial Screening

Name of Proposal (policy/strategy/function/ service being assessed)	CCG Controlled Environment for Finance (CEfF) Policy
Those involved in assessment:	Policy developed in consultation with the IG, BI & IM&T Steering Group and for endorsement by the Integrated Performance and Assurance Committee
Is this a new proposal?	No
Date of Initial Screening:	July 2015
What are the aims, objectives?	To ensure the effective and lawful management of the CEfF processes within the CCG
Who will benefit?	All staff working for the CCG who are involved in the creation, submission, receipt, validation, or payment of invoices for health care services funded by the NHS and all staff for awareness.
Who are the main stakeholders?	Staff; Managers; IG, BI, IM&T Steering Group
What are the desired outcomes?	Staff awarenenss of the Policy through being advised of its availability on the CCG's website via Staff Comms.
What factors could detract from the desired outcomes?	Lack of awareness of the existence of the Policy; Failure to follow the Policy/procedure.
What factors could contribute to the desired outcomes?	Knowledge of the policy and its implementation.
Who is responsible?	Staff, managers, IG, BI, IM&T Steering Group
Have you consulted on the proposal? If so, with whom? If not, why not?	Policy developed in consultation with the IG, BI & IM&T Steering Group for approval and endorsement by the Integrated Performance and Assurance Committee.

Which protected characteristics could be affected and be disadvantaged by this proposal (Please tick)		Yes	No
Age	Consider: Elderly, or young people		X
Disability	Consider: Physical, visual, aural impairment, Mental or learning difficulties		X
Gender Reassignment	Consider: Transsexual people who propose to, are doing or have		X

Which protected characteristics could be affected and be disadvantaged by this proposal (Please tick)		Yes	No
	undergone a process of having their sex reassigned		
Marriage and Civil Partnership	Consider: Impact relevant to employment and /or training		X
Pregnancy and maternity	Consider: Pregnancy related matter/illness or maternity leave related mater		X
Race	Consider: Language and cultural factors, include Gypsy and Travellers group		X
Religion and Belief	Consider: Practices of worship, religious or cultural observance, include non-belief		X
Sex /Gender	Consider: Male and Female		X
Sexual Orientation	Consider: Know or perceived orientation		X

What information and evidence do you have about the groups that you have selected above?
The above protected characteristics will have no adverse impact as the Policy has been developed in accordance with new Data Protection legislation (ie General Data Protection Regulation May 2018).

Consider: Demographic data, performance information, recommendations of internal and external inspections and audits, complaints information, JNSA, ethnicity data, audits, service user data, GP registrations, CHD, Diabetes registers and public engagement/consultation results etc.

How might your proposal impact on the groups identified? For example, you may wish to consider what impact it may have on our stated goals: Improving Access, Promoting Healthy Lifestyles, Reducing Health Inequalities, Supporting Vulnerable People

Examples of impact are given below:

- Moving a GP practice, which may have an impact on people with limited mobility/access to transport etc
- Planning to extend access to contraceptive services in primary care without considering how their services may be accessed by lesbian, gay, bi-sexual and transgender people.
- Closure or redesign of a service that is used by people who may not have English as a first language and may be excluded from normal communication routes.
- Please list the positive and negative impacts you have identified in the summary table on the following page.

Summary	
Positive impacts (note the groups affected)	Negative impacts (note the groups affected)
N/A	N/A

Summarise the negative impacts for each group:
N/A

What consultation has taken place or is planned with each of the identified groups?
The Policy was developed and approved in consultation with the IG, BI & IM&T Steering Group prior to endorsement by the Integrated Performance and Assurance Committee.

What was the outcome of the consultation undertaken?
Approval and endorsement sought

What changes or actions do you propose to make or take as a result of research and/or consultation?

Briefly describe the actions then please insert actions to be taken on to the given Improvement Plan template provided.
The Information Governance Team on behalf of the IG, BI and IM&T Steering Group will be responsible for ensuring that this policy is implemented, including any supporting guidance and training deemed necessary to support the implementation, and for monitoring and providing Governing Body assurance in this respect.

Will the planned changes to the proposal?	Yes	No
Lower the negative impact?	N/A	
Ensure that the negative impact is legal under anti-discriminatory law?	N/A	
Provide an opportunity to promote equality, equal opportunity and improve relations i.e. a positive impact?	N/A	

Taking into account the views of the groups consulted and the available evidence, please clearly state the risks associated with the proposal, weighed against the benefits.
Information risk - The CCG must respect patient confidentiality in accordance with the NHS Constitution, ICO Guidance, and the Statutory Code of Practice. 'Necessity' is a qualifying condition to justify the lawful use of PCD.

What monitoring/evaluation/review systems have been put in place?
Monitoring will be undertaken by the Information Governance team. The frequency of review will be every other year or as required.

When will it be reviewed?
July 2023 or earlier if significant change to local or national requirements

Date completed:	2nd July 2021
Signature:	Information Governance Manager
Approved by:	OD & HR Advisor (Equality and Diversity)
Date approved:	15th July 2021

Appendix 1 – Named Staff Access to demographic systems within the CEfF

The organisation will maintain a local staff list of staff members requiring access to GP Registration data and patient demographic information for the purpose of validating invoices with a list of named roles and the systems required to undertake validation.

Responsibility for the accuracy of this list will rest with the Finance Manager

NB: There can be no more than THREE individuals will access to patient data for the purpose of invoice validation at any one time.

Ref	Name	Job role	Date joining CEfF	CEfF Email (capccg.ceff@nhs.net) UUID (Smartcard Number)	SYSTEM ACCESS						Date access ceased
					SPINE (PDS) Portal to enable SCR access	Open Exeter	SCRa3	DBS4	SUS	Other (please note)	

Appendix 2 – Assurance that CEfF staff understand their responsibilities

To provide assurance that staff with access to patient data systems understand their responsibilities. Staff with access to GP registration data and patient demographic information will ensure that they have:

Read and understood the 'Who Pays' Information Governance guidance
Read and the confidentiality clauses contained within their contract of employment

Undertaken mandatory Data Security Awareness Training via the online training tool or using locally provided training material annually including the completion of any role specific modules assigned to them.

Name	
Signature	
Dated	

Appendix 3 - CEfF Backing Data Sets Approved for Inclusion

Data Item	Example	Purpose	Justification
Invoice Number	Not PCD	Identifies the relevant invoice and allows associated with backing data	To enable backing data to be matched with the relevant invoice
NHS Number	NHS Number	The unique identifier for the patient	Needed to determine if the individual is the responsibility of the commissioner
Unique Patient Event identifier	Hospital Provider Spell Number/AE or OP Attendance identifier unique within Provider for the patient event	To ensure the same episode of care isn't paid for by the commissioner more than once. For example, a patient may have several attendances of treatment on the same day.	To distinguish between multiple events carried out for a particular patient on the same day.
Unique Patient Identifier	Local Patient Identifier, GP Practice identifier	To ensure any issue or payment is attributed to the same patient	To identify the individual to the healthcare provider. Particularly as NHS Number is not always known by the provider.
Geographical Locator (identifying location)	Post Code, Lower Layer Super Output Area (LSOA)or Middle Layer Super Output Areas (MSOA)	To resolve issues around services not commissioned via GP or CCG route. Note this is not required in all instances but may be part of a challenge process. Where a Unique Patient Identifier cannot be used or is not relevant.	An NHS Number is not, currently, always present and geographical location is an alternative means of identifying the relevant commissioner. This is required for identifying the usual residence of patients
Provider Details	Organisation Data Service (ODS)6 code of provider submitting invoice related to backing data. IF an ODS code not known then Name of provider as displayed on Invoice	To identify who requires reimbursement for the treatment already provided.	Required to match activity, to provider and ensure payment
Point of Delivery	Outpatient, Emergency Admission, Day Case Admission, Maternity, Accident and Emergency	Required in some circumstances to judge that the requested price/payment noted by the provider complies with PBR or local tariff arrangements for that	Required to match activity and appropriate tariff.

Data Item	Example	Purpose	Justification
		type of patient care event, delivered in this point of deliver setting.	
Relevant date of treatment	Admission Date and Discharge Date of IP Admissions; Arrival Date for AE and Appointment Date for OP.	To identify the relevant commissioner at the point of payment (as outlined in guidance). This may be a period of treatment or the date of attendance and will vary with circumstances.	Date of treatment will help determine the relevant commissioner, especially when the patient moves or circumstances change. It is also used to assess the relevant tariff.
Relevant GP's ODS Code (identifying the relevant and unique GP practice)	SUS Derived Practice	To ensure that the appropriate commissioner is identified. This identifies the approximate location of the patient and the fact they are in receipt of medical care	As CCG are required to pay for those patients, they have responsibility for (as outlined in Health and Social care Act, s13). Identifying the relevant practice helps to determine the relevant commissioner.
Description of service (for example, oncology or radiology which may indicate the patient's condition)	Oncology	To identify the treatment and source of the invoice, to facilitate any challenges	Describes service or location to identify point of challenge
Description of treatment (Clinical Code, written description)	Clinical Code	To identify the treatment and attribute the appropriate cost or schedule	Identifies activity
Description of Prescribed drug	Drug	To identify the prescribed drug	To identify tariff of commissioner (for example, those determined by NICE Guidelines) and whether prescription is justified, or a non-brand alternative is available.

Appendix 4 - Removal of Non-PO Invoices Containing Identifiable Data

NHS SBS and NHS England have worked together on a new function to improve the identification and removal of Non-PO Invoices containing Personal Confidential / Patient Identifiable Data (PID/PCD).

If PID / PCD is found to be included anywhere on an invoice in the Non-PO workflow, users are now able to return the invoice to NHS SBS for action by checking the 'Unable to Process' option and selecting one of the return options as below:

Option	Action Taken/Required
Personal Identifiable Data (PID) on invoice image, please delete and cancel	If this option is selected, the requester will need to contact the supplier requesting a resubmission of the invoice without the PID/PCD. NHS SBS will remove the image and Cancel the document in Oracle.
Personal Identifiable on Backing Document, please remove page and return	If this option is selected NHS SBS will remove the Backing Documentation from the image and return the invoice to the requester for coding and approval.
Personal Identifiable Data on Paper Clip, please remove attachment and return.	If this option is selected NHS will remove the attachment and return the invoice to the requester for coding and approval.

Source: NHS Shared Business Services
https://www.england.nhs.uk/wp-content/uploads/2013/11/New-rejection-mechanism-on-ISFE.pdf