NHS
Cornwall and
Isles of Scilly

Controlled environment for finance policy

Date approved: 27 March 2023

NHS Cornwall and Isles of Scilly Integrated Care Board

Call us on 01726 627 800
Email us at ciosicb.contactus@nhs.net
Visit our website: cios.icb.nhs.uk

Part 2S, Chy Trevail,
Beacon Technology Park,
Dunmere Road,
Bodmin, PL31 2FR
Chair: John Govett
Chief executive officer: Kate Shields

Document control

Title of document: Controlled environment for finance policy
Lead directorate: Finance
Lead team: Finance
Document type: Policy
Subject category: Information
Author(s) name: Sarah Foster, Deputy director finance and commercial services
Date ratified: 27 March 2023
Ratified by: Simon Gittoes-Davies, Chief finance officer
Review frequency: 3 years
To be reviewed by date: 27 March 2026
Target audience: All staff
Can this policy be released under FOI? Yes
Give reasons for exemption if no: N/A

Version control

Version number	Revision date	Revision by	Nature of revisions
V1.0	1 July 2022	ICB	Adopted by NHS Cornwall and Isles of Scilly ICB
V2.0	4 March 2023	Sarah Foster	Refreshed following review
V2.0	27 March 2023	Chief finance officer	Ratification by the Chief finance officer
V2.1	29 March 2023	Corporate governance team	Governance check – amendments made to job titles

You can request any document published on our website in alternative formats. Email our engagement team for more information.

Contents

1. Introduction 5
2. Purpose 5
3. Definitions 6
   - Accredited safe haven (ASH) 6
   - Anonymisation 7
   - Backing data 7
   - Commissioning data set 7
   - Confidentiality advisory group (CAG) 7
   - Consent 7
   - Controlled environment for finance 7
   - Data controller 8
   - Data processor 8
   - Data services for commissioners regional offices 8
   - Health and Social Care Act 2012 8
   - Information governance 8
   - Integrated single finance environment 8
   - Invoice 9
   - Legal bases 9
   - Necessity 9
   - NHS Digital 9
   - NHS Shared Business Services 9
   - Payment by results 9
   - Personal confidential data (PCD) 9
   - Privacy notice 10
   - Processing 10
   - Pseudonymisation 10
   - Public interest test 10
   - Section 251 (NHS Act 2006) 11
   - Sensitive (special category) data 11
   - Weakly pseudonymised data 11
4. Responsibilities 11
   - ICB Board 11
   - Finance, performance and commissioning committee 11
   - Individuals 12
     - Chief Executive Officer (CEO) 12
     - The Senior Information Risk Officer (SIRO) 12

The Caldicott Guardian 12
Director for strategy, planning and corporate services 12
Head of information governance 12
Deputy director of finance and commercial services 12
Senior finance manager 12
Business information service lead 13
All staff working in the CefF 13
5. Legal and regulatory framework 13
6. Operation of the CEfF 13
Receipt of data 14
Retention periods 15
Cross-matching to determine responsible commissioner 15
How challenges will be responded to 15
Implementation plans and monitoring effectiveness 15
Update and review 16
7. Policies referred to in this document 16
Appendix 1: Named staff access to demographic systems within the CEfF 17
Appendix 2: Assurance that CefF staff understand their responsibilities 18
Appendix 3: CefF backing data sets approved by inclusion 19
Appendix 4: Removal of non-PO invoices containing identifiable data 22
Appendix 5: Equality impact assessment 23
Aims, objectives and purpose of the policy 23
Differential impacts 23
Human rights values 24
Public Sector Social Value Act 2012 25
Equality impact assessment action plan 26

1. Introduction

NHS Cornwall and Isles of Scilly (CIoS) Integrated Care Board (lCB) recognises the need for an appropriate balance between openness and confidentiality in the management and use of information. The ICB 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 ICB also recognises the need to share information with other health organisations and agencies in a controlled manner consistent with legislative requirements.

The Secretary of State for Health has approved the NHS England application for an extension for support under regulation 5 of the health service (control of patient information) regulations 2002 (section 251 support). This allows Integrated Care Boards and commissioning support units (CSUs) to process personal confidential data (PCD) which are required for invoice validation purposes.

The approval is subject to a set of conditions, this policy has been written to outline how the ICB is working within this framework and the steps that have been taken to enable the invoice validation processes to be administered lawfully.

The confidentiality advisory group (CAG) reference to approve the extension of S251 support for invoice validation

2. Purpose

The NHS England guidance: who pays? Determining responsibility for payments to providers helps ICBs 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 ICBs do not have a legal right to access 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 ICB 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 ICB 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 ICB will use anonymised or pseudonymised data to validate invoices and this principle applies to all invoice validation activity.

In the majority of instances, the lawful basis to use PCD for invoice validation will be S251 but for individual, patient centred service (for example individual funding requests, personal health budget, continuing health care) the lawful basis will be consent.

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

Although this policy is only directly applicable to staff working within the controlled environment for finance (CEfF), it is still relevant to all staff working for the ICB 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 4 staff can sit within the CEfF environment. These had been nominated by the ICB.

3. Definitions

Accredited safe haven (ASH)

Established in either a ICB or 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, for example identification is not likely to take place.

Backing data

Activity information provided with a copy of the invoice to the ICB 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

Commissioning data sets form the basis of data on activity carried out by organisations that is reported centrally for monitoring and payment purposes. These datasets supports the current version of the healthcare resource group used for the calculation of payment and monitoring of services.

Confidentiality advisory group (CAG)

The CAG is an independent body which provides expert advice on the use of confidential patient information – including providing advice to the Health Research Authority. 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 ICB must keep a record of consent if given. Consent cannot be taken for 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

The CEfF was a new concept established by the section 251 approval as a temporary measure to assist ICBs 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 General Data Protection Regulations(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

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

The Health and Social Care Act 2012 amended the NHS Act 2006 and established ICBs 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

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

NHS England and NHS Shared Business Services have introduced a new mechanism within the integrated single finance environment system, which identifies suppliers, and their associated commissioners, that submit PCD for invoice validation purposes. The ICB is responsible for ensuring that the correct process is followed for the submission of PCD to validate invoices via the ICB's nominated 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 ICB responsible for that patient.

Legal bases

Consent is just 1 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 ICB's privacy 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

The Health and Social Care Information Centre, now known as NHS Digital, was set up as an executive non-departmental public body in April 2013. The functions and duties of the NHS Digital 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

Please visit the NHS Shared Business Services website for further information:

Payment by results

Payment by results is the national 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 2 fundamental features of payment by results 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, persona'

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 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 notice

Individuals should know and understand how their information is used and shared, there should be no surprises. We do this by posting a privacy 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.

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

Pseudonymisation 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 pseudonymised 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 PCD 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 1 strong item (for example 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 ICB 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

ICB Board

The ICB Board is a statutory NHS organisation which is responsible for developing a plan for meeting the health needs of the population, managing the NHS budget and arranging for the provision of health services in a geographical area. The board ensure that the ICB has arrangements in place to exercise its functions effectively, efficiently and economically and in accordance with any generally accepted principles of good governance that are relevant.

Finance, performance and commissioning committee

Chaired by non-executive member (NEM); delegated authority from ICB Board to ratify the CEfF policy and any associated policies and procedures.

Individuals

Chief Executive Officer (CEO)

The CEO has ultimate responsibility for compliance with information governance legislations and guidance.

The Senior Information Risk Officer (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 CEO 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

Director for strategy, planning and corporate services

The director for strategy, planning and corporate services is responsible for advising on information governance strategic direction, the development of policy and guidance for the ICB.

Head of information governance

The information governance manager is 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 finance and performance committee assurance in this respect.

Deputy director of finance and commercial services

The deputy director of finance and commercial services will be responsible for authorisation of staff access to the CefF.

Senior finance manager

The senior finance manager is responsible for ensuring that staff who have access to the CEfF to validate invoices, have received the appropriate training. Staff who are given access to patient data systems for the purpose of invoice validation sign the form at appendix 5 as assurance of their compliance in completing their annual mandatory information governance training and understand their responsibilities around confidentiality with regards to accessing the systems.

Business information service lead

The business information service lead is the designated individual who manages access requests for the CEfF. A log of named access to demographics systems within the CEfF is kept ensuring that only 4 members of staff have access at any 1 time (appendix 1).

All staff working in the CefF

All employees and anyone working on behalf of the ICB, 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 ICB and where relevant of their profession. Everyone has a duty to respect a data subjects rights to confidentiality.

5. Legal and regulatory framework

The section 251 approvals are time-limited and are subject to conditions that the ICB 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 22 November 2013. The ICB completes an assurance statement which is submitted to NHS England who holds and publishes a list of approved CEfF on their own web pages. NHS England and NHS Digital will define the application process, set out the standards expected, and provide detailed information about these conditions.

The ICB 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 ICB 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 PCD within:

- the GDPR and Data Protection Act 2018
- 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
- a secure (restricted) location within the ICB's network
- a specified and limited number of individuals with access to this information

In the case of the ICB, we have been approved for 4 individuals with access to patient information for the purposes of the CefF.

Receipt of data

The invoice is uploaded to Oracle by NHS Shared Business Services. Where possible, NHS Shared Business Services will stop any invoices received by them that contain patient data.

The invoice comes into the workflow of the ICB.

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.

If patient identifiable data (PID) or PCD is found to be included anywhere on an invoice in the non-PO workflow, users are able to return the invoice to NHS Shared Business Services for action by checking the unable to process option and selecting 1 of the return options in Appendix 4.

The provider is advised that the invoice has been cancelled and that it should be resubmitted without containing PID.

The invoice is logged into a spreadsheet register.

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.

The backing data is in the form of a spreadsheet containing GP and postcode data along with NHS numbers and patient identifiers.

Backing data is saved to a secure folder within a restricted site with the provider's name and deleted from the CEfF inbox.

Once the backing information has been received and reviewed against the invoice, the invoice is either accepted or challenged.

Where challenged, the invoice the invoice is queried and put on hold pending resolution with the provider.

Where accepted, the invoice is coded and checked on Oracle then submitted.

The invoice is forwarded to the budget holder for approval.

Retention periods

- The backing information received into the CEfF email address should be deleted as soon as the information is saved into the designated restricted folder.
- Information contained within the restricted folder is reviewed and securely deleted after 6 years to prevent double charging and in accordance with the ICB's records management policy.
- This will be a rolling year on resolved backing only, any unresolved data will be kept until resolved.

Cross-matching to determine responsible commissioner

- The data normally comes through with an invoice number on it or will state the month of the activity.
- The CEfF team will then match with the invoice once received.
- The total of activity must match the amount of the invoice and description.
- The CEfF team then validates the data by ensuring that the NHS numbers belong to patients who were registered to a Cornish GP at the time of the activity that the charges are correct.

How challenges will be responded to

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

Implementation plans and monitoring effectiveness

All employees who have access to the information provided via the CEfF will be required to have read the who pay's advice.

Each member of the CEfF team:

- is required to have read the confidentiality clauses in the general contract of employment
- 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
- 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

In addition to data security awareness training, CEfF staff will refresh their knowledge of CEfF conditions of operation.

It is the responsibility of the senior finance manager to ensure that all CEfF staff have completed these requirements and have signed the proforma within appendix 2 of this procedure.

Update and review

This policy should be reviewed on a 3 year rolling programme and as legislation changes.

7. Policies referred to in this document

This policy should be read in conjunction with:

- Data protection policy
- Pseudonymisation policy
- Records Management Code of Practice for Health and Social Care 2016

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 business information service lead

There can be no more than 4 individuals will access to patient data for the purpose of invoice validation at any 1 time.

Ref	Name	Job role	Date joining CEfF	CefF email: UUID (smartcard number)	Spine (PDS)	Open Exeter	SUS	Other	Other	Date access ceased
1										
2										
3										
4										

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 guidance
- read 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

CefF access

Name: Click here to enter text.
Title: Click here to enter text.
Date: Click here to enter text.

Signature:

Authorised by

Title: Click here to enter text.
Date: Click here to enter text.

Signature:

Appendix 3: CefF backing data sets approved by inclusion

Date item	Example	Purpose	Justification
Invoice number	Not PCD	Identifies the relevant invoice and associated backing data quoting the invoice number.	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/emergency care (AE) or outpatient (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 or middle layer super output areas	To resolve issues around services not commissioned via GP or ICB 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 6 code of provider submitting invoice related to backing data. If an organisation 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

Date item	Example	Purpose	Justification
Point of delivery	Outpatient, emergency admission, day case admission, maternity or emergency department	Required in some circumstances to judge that the requested price or payment noted by the provider complies with PBR or local tariff arrangements for that type of patient care event, delivered in this point of deliver setting.	Required to match activity and appropriate tariff
Relevant date of treatment	Admission date and discharge date of inpatient (IP) admissions; arrival date for emergency care (AE) and appointment date for outpatient (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 ICB's 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	Oncology or radiology which may indicate the patient's condition	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	To identify the treatment and attribute the appropriate cost or schedule	Identifies activity

Date item	Example	Purpose	Justification
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 Shared Business Services and NHS England have worked together on a new function to improve the identification and removal of non-PO Invoices containing PCD or PID.

If PID or 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 Shared Business Services for action by checking the 'unable to process' option and selecting 1 of the return options as below:

Option	Action to be taken
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 or PCD. NHS Shared Business Services 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 Shared Business Services will remove the backing documentation from the image and return the invoice to the requester for coding and approval.
PID 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

Appendix 5: Equality impact assessment

Name of policy or service to be assessed: Controlled Environment for Finance (CEfF) policy
Department or section: Finance
Date of assessment: 15 March 2023
Person(s) responsible for the assessment: Sarah Foster, deputy director finance and commercial services
Is this a new or existing policy? New

Aims, objectives and purpose of the policy

Describe the aims, objectives and purpose of the policy
To ensure the effective and lawful management of the CEfF processes within the ICB.

Who is intended to benefit from this policy, and in what way?
All staff working for the ICB 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.

What outcomes are wanted from this policy?
Knowledge of the policy and its implementation.

What factors/ forces could contribute or detract from the outcomes?
N/A

Who are the main stakeholders in relation to the policy?
Information, Intelligence and Insights Team. Corporate Finance Team

Who implements the policy, and who is responsible for the policy?
Information, Intelligence and Insights Team. Corporate Finance Team

Differential impacts

Does this have a positive or negative impact on people from an ethnic minority background? How will any negative impact be mitigated?
None. N/A

Does this have a positive or negative impact on people who identify as male, female or intersex? How will any negative impact be mitigated?
None. N/A

What is the positive or negative differential impact on people from the perspective of disability?
None. N/A

Does this have a positive or negative impact on people who identify as heterosexual, lesbian, gay, bisexual, pansexual or asexual? How will any negative impact be mitigated?
None. N/A

What is the positive or negative differential impact on people from the perspective of age? How will any negative impact be mitigated?
None. N/A

What is the positive or negative differential impact on people from the perspective of religion or belief? How will any negative impact be mitigated?
None. N/A

What is the positive or negative differential impact on people from the perspective of marriage and civil partnership? This is particularly relevant for employment policies. How will any negative impact be mitigated?
None. N/A

Does this have a positive or negative impact on people who identify as trans or transgender, non-binary, or gender fluid? How will any negative impact be mitigated?
None. N/A

Does this have a positive or negative impact on people who are pregnant, breast feeding mothers, or those on maternity leave? How will any negative impact be mitigated?
None. N/A

Are they any other identified groups? How will any negative impact be mitigated?
None. N/A

Human rights values

How have the core human rights values of fairness, respect, equality, dignity and autonomy been considered in the formulation of this policy/ service/ strategy?
If they have not, please reconsider the document and amend to incorporate these values.

Which of the human rights articles does this document impact?

☐ To life
☐ Not to be tortured or treated in an inhuman or degrading way
☐ To liberty and security
☐ To a fair trial
☐ To respect for home and family life, and correspondence
☐ To freedom of thought, conscience and religion
☐ To freedom of expression

☐ To freedom of assembly and association
☐ To marry and found a family
☐ Not to be discriminated against in relation to the enjoyment of any of the rights contained in the European Convention
☐ To peaceful enjoyment of possessions

What existing evidence (either presumed or otherwise) do you have for this?
N/A

How will you ensure that those responsible for implementing the policy are aware of the human rights implications and equipped to deal with them?
N/A

Public Sector Social Value Act 2012

NHS Cornwall and Isles of Scilly Integrated Care Board is committed and obliged to fulfil the requirements of the Public Sector Social Value Act 2012. This Act requires the organisations to consider how services commissioned or procured might improve the economic, social and environmental wellbeing of an area.

Please describe how this will support and contribute to the local system, wider system and community.
N/A

Describe how the policy contributes towards eliminating discrimination, harassment and victimisation.
N/A

Describe how the policy contributes towards advancing equality of opportunity.
N/A

Describe how the policy contributes towards promoting good relations between people with protected characteristics.
N/A

If the differential impacts identified are positive, explain how this policy is legitimate positive action and will improve outcomes, services and/ or the working environment for that group of people.
N/A

Explain what amendments have been made to the policy or mitigating actions have been taken, and when they were made.
N/A

If the negative impacts identified have been unable to be mitigated through amendment to the policy or other mitigating actions, explain what your next steps are using the following equality impact assessment action plan.
N/A

Equality impact assessment action plan

Issues to be addressed	Action required	Responsible person	Timescale for completion	Action taken	Comments
N/A					

Signed (completing officer): Sarah Foster
Date: 15 March 2023
Signed (head of department/section): Simon Gittoes-Davies
Date: 27 March 2023

Please ensure that a signed copy of this form is sent to both the corporate governance team with the policy and the equality and diversity lead.