Staff/User Training – Invoice Validation in Integrated Single finance System (ISFE) in circumstances where Personal Confidential Data ("PCD") may be included in Scanned invoices requiring validation for patient care

1. Applicability

This material is written to support staff with responsibility for the following roles within the Integrated Single Financial System (ISFE):

- NHS_XXX_Non_PO_Invoice_Approval
- NHS_XXX_Non_PO_Invoice_Approval_Superuser

These responsibilities are used for/on behalf of CCGs for:

- Non PO Invoice Workflow allocation
- Invoice Validation/Coding or
- Authorisation for Payment

NHS Staff involved who need to be aware of and follow this process include Finance officers and their colleagues in Provider Management, Contract Management, Continuing Health Care, Personal Health Budgets, Primary Care commissioning, or equivalent roles: and senior managers with workflow supervision or transaction approval responsibilities.

2. Objective

The objective of this training material is to help ensure that:

- The privacy and safety of patients and service users is not compromised through downloadable images containing Personal Confidential Data (PCD) being accessible in ISFE Accounts Payable.
- PCD in invoice images and supporting documents scanned or attached by SBS when received from healthcare providers, is identified and eliminated.

This training document covers two staff competencies:

- Ability to determine clearly whether supplier invoice documentation, as scanned by SBS and viewable in ISFE Accounts Payable Non PO Invoice Approval Workflow, is compliant with Information Governance Guidance and Data Protection law, including awareness of the risks to the patient/service user in loss of privacy and potential vulnerabilities.
- Being able to undertake the necessary actions in ISFE system and communicating with the Provider (supplier) concerned when a scanned image of a provider invoice contains PCD, to have non-compliant images removed from the ISFE system.

A training video is available which also covers the main points detailed in this document : https://youtu.be/PjabiX-YIqs

3. Definition of PCD

- The NHS Act 2006 defines data as being confidential when it identifies someone AND was given in confidence: this can include NHS number which is an identifier: as even though it is not confidential on its own, it is confidential if it is linked to other health information which relates to the health or diagnosis of a patient/service user.
- For the purposes of this ISFE control review, 'personal' includes the legal definition of personal data, but it is adapted to include dead as well as living people and 'confidential' includes both information 'given in confidence' and 'that which is owed a duty of confidence' and is adapted to include 'sensitive' as defined in Data Protection Law.

Types of PCD can therefore include:

- Name of Service User/patient
- and/or NHS number
- and/or any other reference number (such as a National Insurance Number, Bed/Ward locator or Case number) that is not secured in a restricted data base, only accessible on a "Need to Know" basis, i.e. national spine data
- Home Address of the data subject including at any residential or care home whether temporary or permanent.
- **And is provided in combination** with any of the above: details of the treatment, personal services or other support being provided.

For example, an invoice may quote details of a particular Nursing Home and make reference to one or more packages of care, so long as the Provider does not also reference any patient name, NHS Number, or other individual reference which is not held in a secure and access controlled environment.

For operational reasons, it is not possible to build into SBS ISFE automated invoice scanning and document loading processes sufficient controls to prevent PCD from being scanned in the first place. After scanning, the images of provider invoices become visible directly in many parts of the Accounts Payable suite of responsibilities and through BI Tools Reports to a range of staff in SBS and Finance teams, many of whom have no need to view personal confidential data.

4. Table of potential causes of non-compliance

Information contained in Invoice or on supporting Document.	**Compliant/ Non-Compliant**	**Reason**
Patient or service user name	Non-Compliant	The name, combined with other details on the invoice, means that there is potential for someone to deduce or infer personal details or circumstances of a named individual without their valid permission.
Patient or Service User Address	Non-Compliant	The address combined with other details on the invoice and other information readily available to invoice processing staff or in the public domain, makes it easy to identify a potentially vulnerable individual, and could put her/him at risk.
Case reference	Non-Compliant	Unless you can be sure that the case reference is secured in a database or record store that is only accessible to those who have a legitimate need to know, the case reference may be used as a link to other unsecured information (including information held in other systems, indirectly resulting in the name or other PCD being disclosed).

Details of the treatment being provided	Generally compliant	If no other information of a personal identifiable nature is on the invoice or attached supporting information, this is acceptable. However the more detailed the information given on the face of the Provider documentation, the greater is the likelihood of that information being linked to an individual at which it becomes PCD.
Database case reference from a secure database	Compliant, with provisos	For some service users, such as those supported through providers of Continuing Health Care, Funded Nursing care, Joint Packages, Individual Funding Requests and Personal Health Budgets, CCGs will hold IG compliant data indexed with a case reference to a secure database e.g. to help manage individual patient funding eligibility and oversee provider contracts, and to track and forecast costs. If the provider uses such a case reference to support billing this is acceptable on condition that it is not also used for less secure purposes that would compromise PCD. The security and access measures around any such database would have to be assured through the current and any future IG toolkit requirements. – See *Note 1* below.

Note 1: Users must beware of making any off – system notes or local unsecured copies containing PCD such as a quick reference spreadsheet extract containing Patient details outside of local secure processes and controls.

5. Worked Example

The following example is based on a real instance of an invoice sent by a provider through SBS Tradeshift to a CCG: the “electronic” invoice is supported by supplier generated invoice image and supporting schedules. Taken together these pages illustrate many of the points identified in the table above.

Note 2: in this case the whole electronic document constituted three pages in all – the Tradeshift invoice, plus the Supplier’s own system-generated invoice, and a supporting Schedule with a breakdown of costs. Users should review **all pages** of scanned documents.

Note 3 The Provider and CCG name and all actual PCD shown on the original documents have been changed in this example.

Invoice

Any Tradeshift
Supplier

TO

NHS ANY OLD TOWN CCG (ZZZ)

Topcliffe Lane
Phoenix House
Wakefield
WF3 1WE
United Kingdom

VAT Reg. No. :

Tradeshift Global Location Identifier :

FROM

United Kingdom

Tradeshift Global Location Identifier :

INVOICE NUMBER

1234567

ISSUE DATE
12/4/16

CURRENCY
GBP

ITEM ID	DESCRIPTION	QUANTITY	UNIT	UNIT PRICE	TAX	TOTAL GBP EXCL. TAXES
Item 1	Joe Bloggs	1	pcs	847.28	0%	847.28

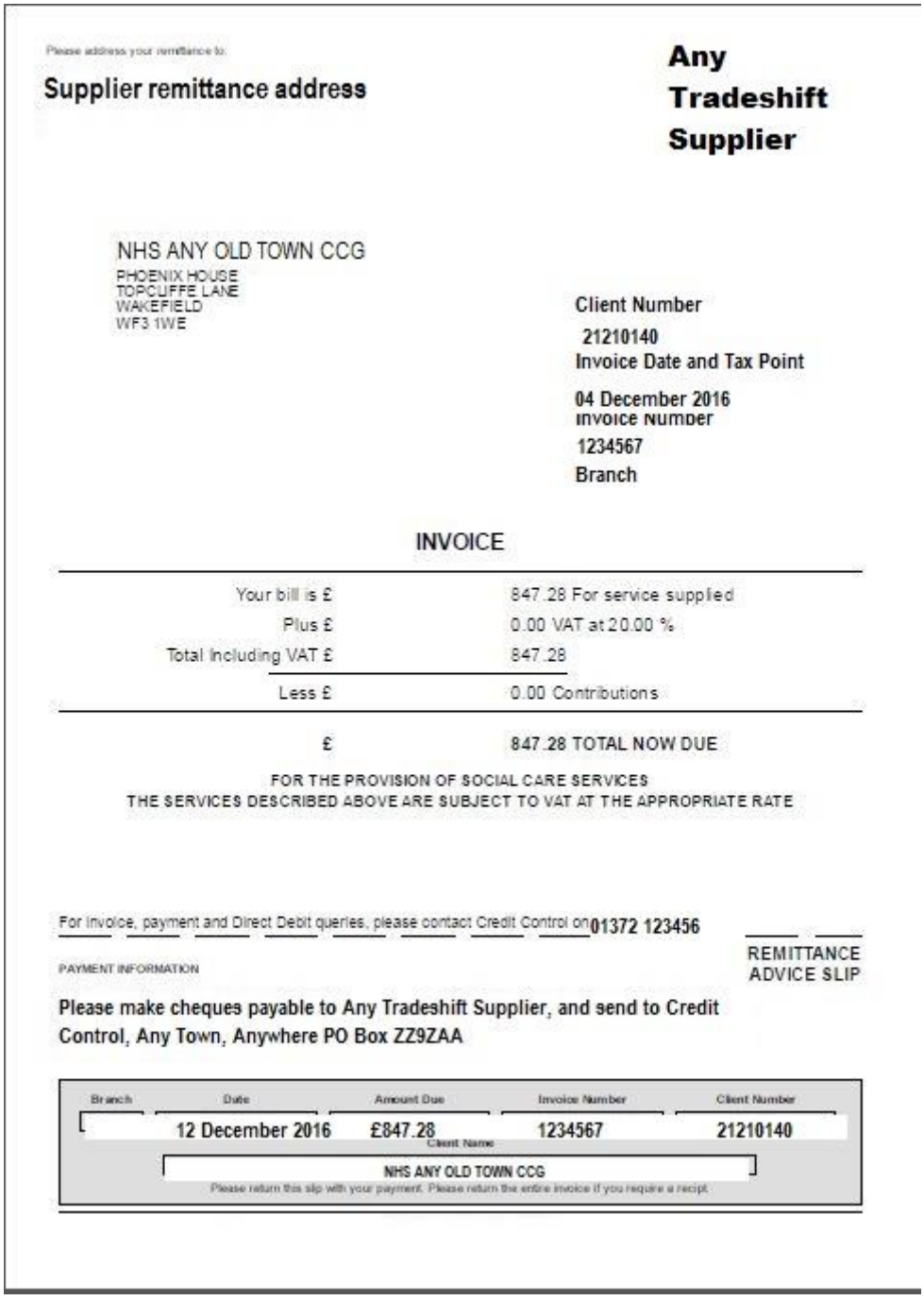
Subtotal excl. taxes **847.28**
GB VAT Exempt 0% *of 847.28 GBP* **0.00**

Total GBP **847.28**
Total taxes GBP 0.00

DELIVERY ADDRESS

United Kingdom

This first page contains one IG breach as the name of the Service user is directly quoted, rather than an acceptable pseudonymised e.g. secure database reference.



Please address your remittance to:

Supplier remittance address

Any Tradeshift Supplier

NHS ANY OLD TOWN CCG
PHOENIX HOUSE
TOPCLIFFE LANE
WAKEFIELD
WF3 1WE

Client Number
21210140
Invoice Date and Tax Point
04 December 2016
Invoice Number
1234567
Branch

INVOICE

Your bill is £	847.28 For service supplied
Plus £	0.00 VAT at 20.00 %
Total Including VAT £	847.28
Less £	0.00 Contributions
£	847.28 TOTAL NOW DUE

FOR THE PROVISION OF SOCIAL CARE SERVICES
THE SERVICES DESCRIBED ABOVE ARE SUBJECT TO VAT AT THE APPROPRIATE RATE

For invoice, payment and Direct Debit queries, please contact Credit Control on 01372 123456

PAYMENT INFORMATION

REMITTANCE ADVICE SLIP

Please make cheques payable to Any Tradeshift Supplier, and send to Credit Control, Any Town, Anywhere PO Box ZZ9ZAA

Branch	Date	Amount Due	Invoice Number	Client Number
	12 December 2016	£847.28	1234567	21210140

Client Name
NHS ANY OLD TOWN CCG

Please return this slip with your payment. Please return the entire invoice if you require a receipt

This second page is the Care provider's own system generated invoice: it is apparently acceptable, as the only reference it contains is a "client number" which, if secured correctly, will enable the invoice to be validated without risk of being linked to the underlying service user's personal details. However the confidentiality of this Client reference must be subject to local risk assessment.

Any Tradeshift Supplier

NHS ANY OLD TOWN CCG

PHOENIX HOUSE
TOPCLIFFE LANE
WAKEFIELD
WF3 1WE

Invoice Date: 4 Dec 2016
Invoice Number: 1234567
Client Number: <no selection>
Team Leader/Care Manager/Group: <no selection>
Cost Code:

SUMMARY & ITEMISED SERVICE

Start Date: 21/11/2016 **End Date:** 27/11/2016

Service Recipient: Joe Bloggs 1 Front Street Anytown
S.S. Case No:

Sheet	Member	Start Date and Time	Grade	Total Care Type	Units	Exp. + Rate/Unit	Total Travel	Client Ex VAT	Contrib.
Week Commencing:	21/11/2016								
TV068843	J Smith	21/11/2016		<no selection>	0.50	15.950000	0.00	7.98	0.00
TV068843	J Smith	25/11/2016		<no selection>	0.50	15.950000	0.00	7.98	0.00
TV068843	J Smith	25/11/2016		<no selection>	7.00	15.950000	0.00	111.65	0.00
TV068843	J Smith	24/11/2016		<no selection>	5.00	15.950000	0.00	79.75	0.00
TV068843	J Smith	21/11/2016		<no selection>	0.50	18.500000	0.00	9.25	0.00
TV068843	J Smith	25/11/2016		<no selection>	0.50	18.500000	0.00	9.25	0.00
TV068845	A Other	24/11/2016		<no selection>	10.00	18.500000	0.00	185.00	0.00
TV068845	A Other	25/11/2016		<no selection>	10.00	18.500000	0.00	185.00	0.00
TV068845	A Other	26/11/2016		<no selection>	10.00	18.500000	0.00	185.00	0.00
				Timesheet Totals	44.00		0.00	780.86	0.00
Week Commencing:	27/11/2016								
TV068843		24/11/2016		Mileage	265.58	0.250000	0.00	66.42	0.00
				Timesheet Totals	265.58		0.00	66.42	0.00
				Service User Totals	309.58		0.00	847.28	0.00

The third page of the electronic document illustrates a number of Information Governance problems with inappropriate disclosure of PCD. Although in this case the provider invoicing system appears to contain the functionality needed to be able to quote a (pseudonymised) Client number, this field has evidently not been used and instead the Name and address of the Service Recipient are clearly shown. Another point to note here is that the names of two care workers are given, which is an unnecessary use of their personal confidential data. It is not just patients whose PCD is to be protected!

This document contains an apparent data breach with potentially serious consequences, as it identifies both the name and home address of a (vulnerable?) individual and clearly identifies that he is in receipt of daily home nursing care from other named individuals. In addition to being a Data Protection breach by unnecessary disclosure of PCD , this document (if leaked) could lead to risk of harm, if for example an unauthorised person were to present as a relief nurse out of hours in order to gain easy access as a “trusted person”, perhaps by saying “Jan Smith (identified as one of the Care workers) has asked me to call to see how you are”.

This illustration emphasises the need for all NHS Finance and Provider/Contract Management staff who manage the ISFE Non PO invoice Approval workflow, to process, validate, code or approve such documents to scroll through and review the ***entire*** document and ***any attachments*** for compliance, and not just to look at the first page.

6. Controlled Environment for Finance (CEfF)

Every CCG will have a CEfF in place where a secure office environment and specially trained staff are used for validation of Provider invoices against centrally maintained Data Sets (such as NHS Spine for validation of Non Contract Activity invoices). Where it is not possible to use pseudonymised locally secured data references to support invoice validation for any provider you should consider using the CEfF.

7. How to process non – compliant provider invoices in ISFE

All staff who handle any part of the Non PO invoice approval workflow in ISFE should be aware of this functionality even if their responsibilities do not normally include handling Provider invoices, as the system enables all payables documents to be accessible to any user who has non PO invoice approval responsibility for the CCG concerned.

The process is described at: https://www.england.nhs.uk/ourwork/tsd/ig/in-val/

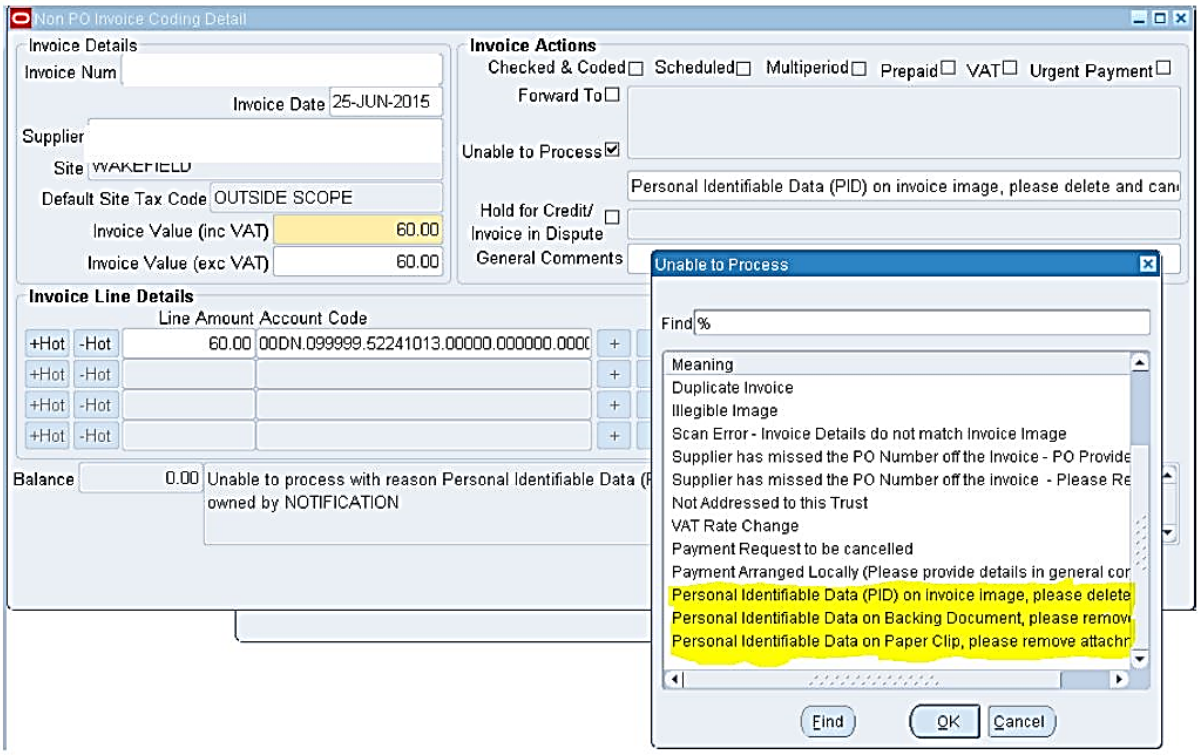
Users must always review the entirety of the scanned document and supporting information

Note 4* "PCD" is the generally accepted abbreviation for "Personal Confidential Data": the SBS process uses a slightly narrower term "Patient Identifiable Data "PID". In practice, for the purposes of the SBS process, these are the same thing, though as illustrated a care worker may also have PCD disclosed wrongly. The following section is the SBS standard process.

SBS process note for invoice rejection or redaction in ISFE on grounds of PCD content

If Patient Identifiable Data is found to be included anywhere on an invoice or scanned attachment in the Non-PO workflow, users must return the invoice to NHS SBS for action by checking the ***'Unable to Process'*** option and selecting one of the return options

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 Provider (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 Data 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 SBS will remove the attachment and return the invoice to the requester for coding and approval. In addition to the System Actions, it is important always to follow up with the invoicing department at the supplier to improve their invoicing practice. You may have local processes in place to do this directly, or through the Information Governance or Finance lead. You may also have local processes in place for incident reporting and risk management which can be applied to improve the processes and controls you operate for maintaining the privacy and integrity your invoice and payment processing The following Screenshot from on PO Invoice approval highlights the three options described above:



Your organisation should have standard template letters available for use to contact suppliers who breach the requirements, or these can be downloaded from the NHS England Website and adapted for local use - https://www.england.nhs.uk/ourwork/tsd/ig/in-val/

8. ISFE "Rules" and other workflow functions to minimise the number of staff who "see" an invoice

Best practice in Provider Invoice management should include the use of ISFE invoice "Rules" to minimise the need for manual redirection of workflow, and so reduce the number of NHS staff interventions in workflow.

- Local finance accounting / services teams can set up and maintain these system rules that essentially filter the invoice based on the CCG and Provider details and automatically direct the invoice in workflow to the correct predetermined manager for validation.

All staff involved in or with responsibility for ISFE Invoice management validation and approval should ensure they apply "Vacation Rules" when out of the office for more than a few days.

- Vacation rules will avoid unintended "timeout" escalations to supervisors and managers through the ISFE invoice non PO invoice automated workflow again reducing invoice visibility and the number of manual interventions.

9. Checklist for completion

Staff who complete this training should be able to:

- Review invoice images loaded in to ISFE for patient care (and any attachments) fully with an understanding of what pseudonymised data is acceptable for invoice validation, and when PCD needs to be rejected.
- Use ISFE Reject Functionality where PCD is disclosed, using the SBS process appropriately either to ask for redaction of details or outright rejection of invoice.
- Contact suppliers directly or through a manager or supervisor to advise of the reason for delay or rejection of an invoice and to support improvements in invoicing practice.
- Have an appreciation of the CEfF processes where more secure invoice validation is needed
- Assist in local monitoring and quality assurance on the satisfactory operation of and compliance with the PCD reject process.
- Use ISFE system functionality to minimise the number of people involved in invoice workflow management for any particular.
- Access national standard materials and guidance to support provider invoice validation where individual care is involved.