

Welcome to the **tenth** edition of the information governance bulletin



Our regular bulletin about information governance and the work of the IG taskforce

Publication Gateway Reference: 01028

10 Information Governance Bulletin



In this Edition...

Page 2:
Welcome to the newly designed bulletin.

Page 3:
Information around the arrangements in place for Invoice Validation.

Page 8:
A list of resources which are available and how to access them.

About this Bulletin...

This bulletin sets out the work that NHS England is carrying out on behalf of the NHS to overcome the information governance (IG) issues created by the legal and organisational changes introduced by the Health and Social Care Act 2012.

This bulletin is written for: Anyone who uses data for secondary uses, such as commissioners inside NHS England and within CCGs; data analytics providers, those working in clinical audit, researchers, managers, clinicians, and patients.

Welcome to the 10th edition of the IG bulletin

With invoice validation continuing to make the headlines among the NHS information governance community, we are focusing on this area of work in this edition of the Bulletin. The IG Taskforce is hosting two workshops on the theme of “Who Pays? Invoice Validation advice”. Both workshops will explore how the invoice validation advice will work in practice, and booking details appear below. We are also grateful to Penny Baxter of Greater Manchester CSU for permission to adapt her paper “Information Governance Advice – Section 251 for Invoice Validation” for this edition.

We have had a lot of queries since April 2013, and to help improve the query process we are launching a new on-line query system. We have also brought together in one place many of the links and resources on information governance issues. Please see our article “Querying the System” and the resource list that follows it.

Regular readers may notice that we’ve made some changes to this edition,

most notably the switch to a landscape format, which we believe will make *IG Bulletin* easier to read on tablets and PC screens. We hope these changes meet with your approval.

Stuart A Notholt
Editor

Forthcoming meetings

Roadshows: Who Pays? Invoice Validation advice

The Secretary of State for Health has approved the NHS England application for support under Regulation 5 of the Health Service (Control of Patient Information) Regulations 2002 (Section 251 Support). This allows clinical commissioning groups (CCGs) and commissioning support Units (CSUs) to process the personal confidential data (PCD) required for invoice validation purposes. This approval is subject to a set of conditions. On 5 December 2013, we published advice which explains these conditions and sets the actions that CCGs, CSUs, and providers need to take in order to ensure they are acting lawfully.

Following on from this, we are holding two roadshows whose aim is to provide an overview of the advice, what it means for CCGs, and to allow participants time to work through invoice validation scenarios. The day will close with a Q&A session. There will be subsequent webinars; details of which will follow the roadshows.

The roadshows will be held on the following dates:

- **London (Ambassador Hotel)- Tuesday 21 January 2014. 11:00-16:00 (Lunch included)**
- **Leeds (Novotel Leeds Centre)- Friday 24 January 2014. 11.00-16:00 (Lunch included)**

Spaces are **limited to 100 per roadshow and will be allocated on a first come first served basis**. Please respond to england.dataworkshops@nhs.net to secure a place indicating which roadshow you would like to attend.

The Information Governance Advice for Invoice Validation is available here: <http://www.england.nhs.uk/wp-content/uploads/2013/12/who-pays-advice.pdf>

Information Governance Advice – Section 251 for Invoice Validation

Invoice validation is part of the effective management of health and social care services, ensuring providers are appropriately reimbursed for the care and treatment they deliver to patients. Commissioning processes and tools have tended, prior to 1 April 2013, to rely on the availability of personal confidential data (PCD) to perform invoice validation.

Since the Health and Social Care Act 2012 was established on 1 April 2013, Clinical Commissioning Groups, GPs and Commissioning Support Units have been unable to use PCD for purposes other than direct care. As a result, commissioners have been unable to use PCD for the purpose of invoice validation and found it difficult to satisfy their statutory duties for fiscal probity and to demonstrate scrutiny for public expenditure.

Section 251 approval for invoice validation

The Secretary of State for Health and Social Care has approved NHS England's application for support under Section 251, to establish a temporary lawful basis for 'necessary' PCD to be used to validate invoices.

The section 251 approval establishes a legal basis for the following:

- Implementing a PCD dataset (including NHS number) for invoice 'backing data' – the 'backing data' is separate from the invoice facing page and identifiers cannot be included in the invoice
- Enabling access to systems for checking the PCD backing data and confirming the CCG responsible for payment
- Testing the feasibility of removing the need for PCD for invoice validation purposes
- Developing a minimum PCD dataset that will lead to the development of an information standard for non-Payment-by-Results data sent by providers

to non-contracting
commissioners

It is important to note that the Section 251 support for invoice validation is temporary, lasting until **22 November 2014**. During this time, further work will need to be completed to design and implement new systems and process to validate invoices using pseudonymised data.

Please note the Section 251 only applies to organisations that have achieved Accredited Safe Haven (ASH) Stage 1 accreditation. If you wish for the CCG to obtain ASH Stage 1 please contact your Information Governance Lead. Additional information on ASH accreditation can also be found at the link below:

<http://www.hscic.gov.uk/media/12203/Accredited-Safe-Haven-Accreditation-Process-Stage-1---June-2013/pdf/safe-haven-accred-proc-stage->

(Short code:<http://tinyurl.com/o2mqsvf>)

Invoice validation options for a CCG

There are two sets of options available for invoice validation which depends whether the CCG has ASH Stage 1 accreditation or not. These are detailed in the table below. Please note a CCG may now decide to apply for ASH Stage 1 if it so wishes to use the set of options available to them in the second column for invoice validation.

For CCGs who do not have ASH Stage 1 accreditation

- Where a CCG is already validating invoices without the need to use PCD, this process is lawful and can continue
- Where the CCG currently uses the DSCRO to validate invoices, this can continue.
- The CCG may also choose to use their CSU's CEfF (Controlled Environment for Finance) to receive PCD backing data and validate invoices

For CCGs who have ASH Stage 1 accreditation

- DSCROs can flow weakly pseudonymised data into a CCG's Controlled Environment for Finance (CEfF) – definition of a CEfF is below
- CCG can undertake invoice validation within the CCG's CEfF by using a backing data set included with the invoice – definition of backing data set is below

CCG can have invoice validation undertaken within the CSU's CEfF by using a backing data set included with an invoice

Definitions

Controlled Environment for Finance (CEfF)

A CCG or CSU must establish a 'controlled environment for finance' (CEfF) before it can receive invoice backing data. This is a new concept and has been established as an interim solution to allow necessary PCD to be received and used for

invoice validation purposes within a CCG or CSU.

A CSU or CCG that has achieved ASH Stage 1 accreditation will be eligible to apply for CEfF accreditation. A statement of compliance for CEfF is being developed and further details of the application process will be published shortly.

ASH Stage 1 and CEfF organisations need to maintain appropriate segregation of staff and systems. PCD should not be passed to other parts of the organisation without a supporting legal basis. Robust technical and organisational security controls will be required to separate CEfF staff and processes from other CCG or CSU staff to ensure the protection of PCD.

Setting up a CEfF involves:

- Separating staff for invoice validation from other staff
- Technical and physical isolation of PCD
- Creating a secure central point of contact directly into the CEfF for receiving PCD backing data securely – to be registered with NHS England

- Establishing access controls (i.e. smartcard, role-based access controls.)

Backing data

Activity information provided with a copy of the invoice to the CCG or GMCSU CEfF to evidence that the health care services delivered and amount of payment claimed either under a commissioning contract or under a non-contract agreement. Further information regarding this can be found in [Who Pays? Information Governance Advice for Invoice Validation at
http://www.england.nhs.uk/wp-content/uploads/2013/12/who-pays-advice.pdf](http://www.england.nhs.uk/wp-content/uploads/2013/12/who-pays-advice.pdf)

Short Code: <http://tinyurl.com/oeub3r7>

Responsibilities

Working with providers

CCGs and CSU will work with providers to explain their requirements for invoicing and backing data and to implement the changes to ensure that:

- PCD is not included on the invoice facing page
- The invoice is submitted to NHS Shared Business Services
- The approved PCD data sets are included on the backing data and sent directly to the appropriate secure contact point
- The invoice number is included on the backing data to provide a link between the two sections
- The backing data and a copy of the invoice are submitted to the single secure point of contact provided by the CCG or CSU

A secure contact point must be established for providers to submit backing data and copy invoices to the CEfF of the CCG or CSU. This contact point will need to be communicated to providers and to NHS SBS, and be registered with NHS England.

The CCG or CSU is responsible for informing the provider if they disagree with the allocation of the CCG responsible for paying the invoice and to explain the reason why they do not consider the patient to be their responsibility; for instance:

- The patient is registered with a GP practice that is not a member of the CCG
- The patient has moved to a postcode that is not in the area of residence covered by the CCG member practices
- The treatment is specialised and is the responsibility of NHS England

The submission of PCD backing data to the wrong CCG or CSU is a personal data breach.

CCGs and CSUs need to design systems to capture, report, investigate and manage personal data breaches.

Role of Data Services for Commissioners Regional Officers (DSCROs):

The delivery units of Data Services for Commissioners Regional Officers (DSCRO) will continue to process service level agreement monitoring data for CCGs and raise patient registration challenges with providers on behalf of CCGs. The standard output from DSCROs will continue to be pseudonymised.

If a CCG has achieved ASH Stage 1 accreditation, and has a CEfF in place,

the DSCRO can provide weakly pseudonymised data.

Responsibility of the provider:

The provider is responsible for determining the commissioner of each activity to ensure that the correct commissioner is identified on both the invoice and on the backing data. Providers have to ensure that any PCD is included only in the backing data section of the invoice. The invoice number should be included on both the invoice and backing data and will be used as the non-identifiable unique number for reference and aligning purposes.

The NHS number is an identifier and should be regarded as PCD. It must not be used within the invoice and it is not acceptable to use the NHS number for aligning invoices with the relevant backing data.

The original invoice should be submitted to NHS SBS and cannot include any PCD, therefore, the backing data must *not* be sent to SBS. The provider also submits a copy of the invoice, including the backing data, to the CCG identified as the commissioner responsible for payment, providing that organisation

has a secure contact point registered with NHS England – further information on this process will be communicated when available.

Exemptions to the Section 251 extension

The use of PCD to validate invoices in the following situations is *not* covered by the Section 251 approval:

- Specialist service commissioned by NHS England
- Payment for healthcare service provided to private patients
- Determining which is the responsible commissioner where care is provided over the border with a devolved administration
- Invoice validation by local authorities or for services jointly commissioned by the NHS and a local authority

NHS England is considering these exemptions and will issue further advice in due course.

Other NHS organisations and independent sector providers, acting as a data processor under contract with a CCG to validate invoices on

their behalf, are not in scope of the Section 251 approval.

Summary

- The extension of the Section 251 approval allows necessary PCD to be used for invoice validation purposes without the need to obtain explicit patient consent for 12 months from 22 November 2013.
- The CCG needs to choose which option it wishes to adopt for invoice validation as highlighted in the “Invoice Validation Options for a CCG” section
- CCGs and CSUs need to establish systems in compliance with this advice to ensure that PCD is processed lawfully and any backing data from a provider that includes necessary PCD evidence to support an invoice must be submitted to the CEfF via the approved secure contact point.
- During this time further work is to be completed to design and implement new systems and processes to validate invoices using pseudonymised data.

- CCGs and CSUs will have to work closely with providers to ensure that this advice is communicated and implemented.

The full NHS England advice can be found at the link below:

www.england.nhs.uk/ourwork/tsd/data-info/ig/in-val

With acknowledgements to Penny Baxter, Data Quality and Information Governance Manager, Greater Manchester Commissioning Support Unit

Querying the system

Generally speaking, the enquiries we receive at NHS England concerning information governance fall into three categories.

A *query* is an enquiry sent to NHS England which can be answered within the context of current policy, work and commitments. Generally a query will be seeking advice, or asking for NHS England's position on various matters.

A *request for information* is where the requestor is asking for information or data held by NHS England, rather than

seeking advice or asking for a position statement. If it can be dealt with easily then this can be responded to.

Otherwise a request for information needs to be treated as a Freedom of Information request. In this case the request will be passed to the Contact Centre in line with NHS England's procedure for FOIA requests. It should be noted that the enquirer does not need to state that they are making a Freedom of Information for it to be treated as such. However, if the request is being treated as a FOIA request the enquirer will be made aware of this and who to contact should follow up be necessary.

Thirdly, there are *issues*. These cannot be answered without further investigation, negotiation or work. To undertake this will require prioritisation and may require a product to answer the query. We are developing a more comprehensive process to help us deal with issues raised and will keep readers informed through this Bulletin.

Lastly, there are also some enquiries that fall outside the scope of what we are able to answer, for example on individual projects, documents or

workstreams that are external to NHS England.

Before submitting a query to NHS England, please take a look at the resource list on page 7 onwards, which has been designed to help you to find the information needed to answer most IG related queries (this page is also available on-line at <http://www.england.nhs.uk/ourwork/tsd/data-info/ig/ig-resources/> (Short code: <http://tinyurl.com/ondlcmj>))

If a query falls outside the information provided on the information resource page, please complete an IG Query Form – available on-line from the address above.

Resource List

Category Number	Description	Short code links	Source
1	Access to Patient Confidential Data (PCD) & s251	http://tinyurl.com/puy7zzh	Health & Social Care Information Centre (HSCIC)
		http://tinyurl.com/ogw3ofo	Health Research Authority
		http://tinyurl.com/oxtqch8	Health & Social Care Information Centre (HSCIC)
2	Accredited Safe Havens (ASH)	http://tinyurl.com/g2ozguw	Health & Social Care Information Centre (HSCIC)
3	Care.data	http://tinyurl.com/jw3wz88	NHS England
4	Clinical Audit	http://tinyurl.com/oy8kh95	NHS England
		http://www.hqip.org.uk/	Healthcare Quality Improvement Partnership
5	Commissioning Data	http://tinyurl.com/puy7zzh	Health & Social Care Information Centre (HSCIC)
6	Consent	http://tinyurl.com/nsu7fpk	NHS Choices

		http://tinyurl.com/nwfr5pl	General Medical Council
		http://tinyurl.com/objl5v5	General Medical Council
		http://tinyurl.com/ptltplu	Medical Protection Society
7	Counter Fraud	http://tinyurl.com/qccucyn	NHS Business Services Authority
8	Definitions	http://tinyurl.com/ob4k4wl	Health & Social Care Information Centre (HSCIC)
9	Disclosure of Records	http://tinyurl.com/pf53qax	NHS England
		http://tinyurl.com/pz2g76a	NHS Choices
		http://tinyurl.com/ph8vsqd	National Archives
10	Fair Processing Notices	http://tinyurl.com/q5kej6g	Information Commissioner's Office
11	IG incidents	http://tinyurl.com/no2zwqn	Health & Social Care Information Centre (HSCIC)
		http://tinyurl.com/ob322vb	Health & Social Care Information Centre (HSCIC)
12	IG structure/IG bulletins	http://tinyurl.com/ne82jvj	NHS England
		http://tinyurl.com/omp462y	NHS England

		http://tinyurl.com/ovkqbag	NHS England
13	IG Toolkit	www.igt.hscic.gov.uk	Health & Social Care Information Centre (HSCIC)
14	IG Training	http://tinyurl.com/o5bdc8b	Connecting for Health
15	Invoice Validation	http://tinyurl.com/gh9gmag	NHS England
16	NHS number	http://tinyurl.com/qd96tej	Health & Social Care Information Centre (HSCIC)
		http://tinyurl.com/olcyfya	Health & Social Care Information Centre (HSCIC)
17	PCT/SHA Legacy (DH Legacy Management Team dealing with legacy issues relating to records etc.)	Email LMTenquires@dh.gsi.gov.uk	DH Legacy team email address
		http://tinyurl.com/ovus2xy	Gov.UK
18	Policy	http://tinyurl.com/pvxluer	NHS England
19	Privacy Impact Assessment	http://tinyurl.com/omf9jxr	Information Commissioner's Office
20	Public Interest disclosure of information	http://tinyurl.com/nn5kj8z	Gov.UK
21	Records Management	http://tinyurl.com/pf53qax	NHS England

		http://tinyurl.com/nsk3orn	National Archives
		http://tinyurl.com/ovus2xy	Gov.UK
22	Risk Stratification	http://tinyurl.com/kdbtj22	NHS England
23	Safeguarding	http://tinyurl.com/oblazu2	NHS England
		http://tinyurl.com/oohk9yl	NHS England
24	Social Media	http://tinyurl.com/nmj6bfk	NHS England
		http://tinyurl.com/no6m7yy	Health & Social Care Information Centre (HSCIC)

Integrated Care Modelling

In this feature, we look at three of the key areas with regard to integrated care modelling:

Risk Stratification

Currently, the Section 251 to use identifiable data collected by the Health & Social Care Information (HSCIC) Centre for risk stratification and subsequent re-identification is not permitted. Even once the Secretary of State has approved the principle each solution will need to be reviewed. Proposed solutions will then either be approved to proceed when signing up to a statement of compliance, or required to make changes to meet the criteria set by the Secretary of State. In any case, each local implementation has to demonstrate a commitment to the wider data protection requirements outlined in the existing NHS England risk stratification advice <http://www.england.nhs.uk/wp-content/uploads/2013/06/ig-risk-ccg->

[gp.pdf](#) (See pages 13-15 in particular.)
These commitments include fair

processing of the entire population and managing dissent.

ASH or not an ASH Stage 1

While an organisation may be compliant with the core Accredited Safe Haven (ASH) requirements (namely a compliant IG Toolkit) the HSCIC will not recognise someone as an ASH Stage 1 until the Data Sharing Contract and Data Sharing Agreement have been agreed by all relevant parties. The data can then flow for commissioning purposes, including invoice validation. Re-identification should take place in a Controlled Environment for Finance (CEfF). Until the risk stratification Section 251 approval is granted by the Secretary of State, and the steps outlined are undertaken, the data cannot be used in the clear for risk stratification.

The ASH environment should only have one weak identifier. Usually, this will be the NHS Number. It is not envisaged that there will be a move to the receipt of full Secondary Uses Service data in the ASH. While the Controlled Environments for Finance

(CEfE)s will be able to access additional systems to undertake validation, it should be separated securely from the ASH. Some validation may be able to occur in an ASH where an organisation only needs the NHS Number to validate. This may, for example, be where an ASH has a master patient index (MPI) of registered patients for each clinical commissioning group in a weak pseudonymised form that is used to reconcile against activity data.

Controlled Environment for Finance (CEfF)

Validation using just NHS Numbers in an ASH is possible if the organisation can rely on NHS Numbers. But

generally that has not been the only validation required. The Section 251 in relation to invoice validation is designed to allow for those invoice processes where it cannot be reasonably expected that consent could be obtained by a commissioner or a Commissioning Support Unit on their behalf. The compliance statement for the CEfF should be published shortly, but each organisation that has set one up has done so in line with the Who Pays? Information Governance Advice for invoice validation advice. This uses a data minimisation approach so organisations should only be undertaking searches where it is strictly necessary. This should take place in a documented controlled environment that might be linked to the ASH but where the ability to validate residency would be restricted to a maximum of three people per CCG. The current validation processes operating with the seconded CSU staff to the Data Services for Commissioning Regional Office will be transferred to a CEfF established within the CSU to maintain the current processes. Work is ongoing to implement that within the CSU, but again the process and extent to which the data can be used is limited.

This does not extend to a GP practice validating charges applied to their own patients as this is not how the current NHS Act 2006 has been framed in relation to the functions of a CCG. This is something that has been requested but is not covered under the Section 251 as it wasn't deemed necessary to fulfil the currently framed statutory provisions within the wider legal framework.

Notes and Queries

Q: In 2012 it was agreed to change the policy set by NHS Connecting for Health that prohibited any off-shoring of patient data. Responsibility was moved to individual NHS organisations, to make a judgement on a risk-assessed basis.

Given the obvious sensitivities surrounding off-shoring of patient data, what are the issues that NHS organisations should be considering in this regard?

As with any other disclosure, organisations will need to first assure themselves in two areas:

- The legal basis for the disclosure, either through statute or patient consent
- whether the use of personal or confidential data is necessary for the purpose

In addition, organisations must ensure they consider Data Protection Requirements in relation to countries outside the European Economic Area (EEA) and risk assess the particular circumstances of the disclosure and use of the data in question. However, even if these criteria are met, NHS England has given an undertaking to the Confidentiality Advisory Group that data included in Section 251 support will be retained in the UK. This is the case regardless of whether the data processor is an NHS organisation or a third party provider. Permission to off-shore would therefore need to be obtained from the CAG in relation to data obtained under Section 251 regulations.

In Section 251 terms 'off-shoring' means anywhere outside of England

and Wales. As a rule of thumb, the level of risk outside of England and Wales can be viewed as being in concentric circles:

- Scotland and Northern Ireland: Generally this would be acceptable, provided there is an English sponsor and oversight;
- European Economic Area and other countries recognised by the European Commission as having an equivalent protection regime for data: As with Scotland and Northern Ireland, an appropriate sponsor would be needed and work undertaken to minimise the use of identifiable data;
- Rest of the World: Would need to be risk assessed and assurance obtained in relation to Data Protection Act Principle 8 requirements. In general, it is likely that – even if the CAG found the proposed off-shoring to be acceptable – the degree of oversight required would outweigh any cost saving benefit.

Earlier advice on this topic is available at:

<http://www.connectingforhealth.nhs.uk/systemsandservices/infogov/igsoc/links/offshoring.pdf>

Q: Some GP system providers have been offering practices ‘shared practice’ functions. What are the legal implications of this approach?

The key question that needs to be addressed is whether:

- 1) the practices intend to form a “super practice” (a single legal entity) or
- 2) are maintaining separate legal identities that would, in effect, be making disclosures to every other practice in their “group” or consortium.

A privacy impact assessment will be required to consider how the principles of common law duty of confidentiality and data protection will be satisfied.

If practices are forming a single legal entity, they must inform every patient of this change and what restrictions patients can exercise in relation to data sharing across the different practices. As this is a change in data controllership, individuals have to be informed in advance and given

adequate opportunity to raise concerns or move practice. Consideration should be given to additional access controls to limit access to particular sites to accommodate patient concerns.

This would facilitate the establishment either of shared back office functions or of direct care services, such as a combined Out-of-Office-Hours (OOH) service.

Within a collaborating network or consortium there are a number of models which allow a consent-based model of access and fair processing. For example, a practice might invite patients to attend a neighbouring practice for flu vaccinations when they are closed. However, the notice to that effect should advertise that “the neighbouring practice will not have routine access to records unless you attend and provide consent to access your records. Such access would be via a secure connection and have a full audit trail. Once treatment is carried out, the neighbouring practice will let us know so we can update our records.”

If the practices are maintaining separate legal identities they must

notify every patient of their intention to share records, setting out the purposes of the data sharing and, in the case of back office functions, seek explicit consent as this is not direct care. For OOH services, consent may be implied provided patients have been informed and given adequate opportunity to raise concerns. Access controls should be in place to restrict access to a single practice where a patient does not want their data shared with the other practices.

Please welcome...

Jenny Spiers has recently joined the Task Force as an Information Governance Specialist. Jenny will work four days per week on secondment from Pennine Care NHS Foundation Trust, where she will retain her role as Information Governance Manager one day per week. She has 32 years' experience working in the NHS and twelve in Information Governance, particularly in mental health, specialist services (such as drug and alcohol), community and learning disabilities.



Jenny also chairs the Greater Manchester Information Governance Group and represents the Effective Information Sharing and Security (EISS) Network Leadership group meetings run by iNetwork, working with partners throughout the public sector organisations across the North West and the Information Commissioner's Office.

In the news...

ICO consultation now open

As part of the Information Commissioner's Offices commitment to deliver its regulatory responsibilities as efficiently and effectively as possible, the ICO is reviewing its approach to dealing with the complaints and concerns the public raise under the Data Protection Act (DPA). The consultation on this subject runs until the end of January 2014. The ICO's consultation paper is available at

<http://ico.msgfocus.com/c/13baigSDYuFq1mVtYiqAU>

Data collection

The announcement that the NHS is to start combining patient data from GPs and hospitals for the first time attracted some media interest, with our own Dr Geraint Lewis, the Chief Data Officer for NHS England, being interviewed on a number of channels including the BBC – see

<http://www.bbc.co.uk/news/health-25622337>