## Index

1. [The need for a DPIA – Article 35(1)](#need)
2. [Conflicts of Interest](#conflict)
3. [Documents](#documents)
4. [Timescales and “Deadlines”](#timescale)
5. [Simultaneous new processing](#simultaneous)
6. [Is personal data being processed?](#personal)
7. [The Processing - Article 35(7)(a)](#Art357a)
   1. [How does this directly benefit data subjects?](#bds)
   2. [How does this directly benefit our organisation?](#dboo)
8. [Consultation – Article 35(9)](#consult)
9. Article 35(7)(b) – Necessity and Proportionality
   1. [Common Law](#commonlaw)
   2. [Caldicott Principles](#caldicott)
   3. [The Data Protection Principles – Article 5](#article5)
10. [“No Surprises”](#surprises)
11. [GMC Confidentiality Principles](#GMC)
12. The Human Rights Act 1998
13. [Article 28 – Data Controllership and Data Processors](#article28)
14. [Data Subject Rights](#dsr)
15. Things to think about
    1. [Surrender of control](#surrender)
    2. [Do we have to do disclose?](#have)
    3. [Can we do this in a less intrusive way?](#without)
    4. [Is this lawful?](#lawful)
    5. [Is this ethical and fair?](#ethical)
    6. [Reputational risks](#reputation) & Trust in Doctors
    7. [Consequences of not processing](#notproceeding)
    8. [What about children?](#children)
    9. [How does this compare with other, similar projects?](#compare)
16. [Article 35(7)(c) – Risks to data subjects](#risks)
17. [Article 35(7)(d) - Measures to mitigate risks](#mitigate)
18. [Conclusion](#conclusion)
19. [Sign Off](#signoff)

[Appendix 1 – attached documents](#app1)

## Need for a DPIA - Article 35(1)

This project has several criteria that warrant a DPIA:

* *Processing special category data* – health & social care data
* *Large Scale of special category data* - Article 35(3)(b)
* *Children*
* *Vulnerable adults*
* *Processing that may impact upon data subject rights*
* *Disclosure of information that consumer organisations may already have access to*

It is policy for Oakley Health Group (OHG) to *always* undertake a DPIA for any new, or significant change in an existing, data sharing project involving the personal confidential (and sensitive) information of our patients.

[*Back to Index*](#index)

## Conflicts of interest

Dr Neil Bhatia has no conflicts of interest in undertaking this DPIA, either in his role as IG lead/Caldicott Guardian or as the Data Protection Officer for OHG.

He is neither an employee of, nor receives payment from, the CCG, CSU, SCAS, NHS 111, or any other related organisation.

Any decision to proceed with processing, as a result of the conclusions of this DPIA, will be a partnership decision (majority vote). As a GP partner, however, Dr Neil Bhatia is entitled to a personal vote on this matter.

[*Back to Index*](#index)

## Documents

We have been provided with:

* A proposed Data Sharing Agreement between the two data controllers, OHG and SCAS NHS 111
* A DPIA undertaken by SCW CSU (who is neither a data controller nor a data processor in this arrangement)

[*Back to Index*](#index)

## Timescales and “Deadlines”

*Does additional, related or subsequent processing depend on deciding on this processing by a certain date?*

No – this is a voluntary project and there is no such deadline.

[*Back to Index*](#index)

## Simultaneous new processing

*Is any other data sharing project being launched at the same time, that might lead to confusion for patients?  
Remember when SCR & care.data were launched simultaneously…?*

No, no other data sharing project (whether disclosure or access) is being launched simultaneously.

[*Back to Index*](#index)

## Is personal data being processed?

*Or is this truly anonymous data out with the GDPR/DPA?  
Pseudonymised data = personal data*

This is personal, confidential, special category, data that we are considering granting *access* to.

## Article 35(7)(a)

* **The nature of the processing**

*How will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? You might find it useful to refer to a flow diagram or another way of describing data flows. What types of processing identified as likely high risk are involved?*

*“GP Connect is a NHS Digital project that aims to make information held in GP practice IT systems available right across health and social care, by standardising system integration and simplifying the operating model, using API technology.” (NHS Digital)*

The source of the data is the electronic GP Record (EMIS Web), We would be allowing organisations – initially SCAS NHS 111 – a read-only,   
“on-demand”, and real-time, view of information derived from the GP record, when clinically justified, or clinicians with a legitimate relationship to the patient, and with the explicit permission of the patient.

* **Scope of Processing**

*What is the nature of the data, and does it include special category or criminal offence data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover? What will we learn about people that we already do not know, either by obtaining new information or by combining existing information?*

The data is personal confidential medical data, and so is special category data. The amount visible to the organisation accessing the record, the “consumer organisation”, is detailed in the “*Access record HTML overview of the views*” document available in [Appendix 1](#app1) of this DPIA.

In brief:

◾ Active problems and issues

◾ Current medication issues

◾ Current repeat medications

◾ Current allergies and adverse reactions

◾ Last 3 encounters

* **Context**

*What is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel in any way? What is the current state of technology in this area? Are there any current issues of public concern that you should factor in?*

The information consists of the personal data of our patients. Patients have control over such access in two ways:

* There are *always* asked for “permission to view” their GP record via GP Connect. They can say no at this point
* If they *never* want their information to be accessible in this way, even in an emergency, then they can opt-out completely by requesting that the GP surgery sets their “data sharing” flag within their GP record (EMIS Web) to “do not share”
* **Purposes**

*What do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing for you, and more broadly? What will this processing allow us to do that we cannot do now?*

The sole purpose for GP Connect is to enable information to be available to clinicians working in SCAS NHS 111 (and subsequently, the NHUC GP out-of-hours service and SECAMB) when a patient rings up for advice. As such, this is a *direct medical care* purpose only.

There are no secondary uses of the information available to consuming organisations via GP Connect.

*“GP Connect APIs can only be used legally for direct patient care, not for planning or research.”*NHS Digital

When appropriate, addition clinical information available to the emergency services, and organisations such as NHUC dealing with patients when the surgery is closed, may allow them to better triage and manage the clinical enquiry. Whilst information is already available to the consuming organisations, as will be made clear later on such information is unreliable and temperamental, limited in scope, not “in real time”, generally held in low regard, and may not be available via those routes in the near future.

Access to GP Connect is now built-in to Adastra, as used by both SCAS NHS 111 and NHUC:

*“GP Connect Access Record: HTML is now integrated with the Adastra clinical patient management system. This means 111 and Integrated Urgent Care (IUC) service providers will be able to view a patient’s up-to-date record held by their own GP and given access to a range of important information about a patient including encounters, allergies, medications, referrals and more.”*[NHS Digital](https://digital.nhs.uk/services/gp-connect#consumer-supplier-progress)

### How does this directly benefit data subjects?

*What is the intended outcome for individuals?*  
Better, safer, triage and medical management by organisations out with the GP surgery.

### How does this directly benefit our organisation?

*Does this give us a “competitive advantage”?*  
*"If you just treat privacy as a function of regulatory compliance, you’ll do the bare minimum. Businesses need to think of privacy as a competitive advantage.”*  
Anna Cavoukian, Global Privacy and Security by Design Centre

The expectation is that better, safer, and more appropriate management of our patients out of hours will result in better outcomes for patients, less admissions to hospital unnecessarily, and the potential for patients to be dealt with “completely”, so resulting in less need for such patients to attend their GP surgery the next day.

Promoting access to the GP records:

* in a safe, consensual and transparent way
* for direct care purposes *only*
* when our patients have been informed of such processing
* and where the GP surgery maintains *full* control and oversight of the processing

will be reassuring to our patients and further enforce our standing as a practice that fully upholds the privacy, confidentiality, and data protection of our patients’ GP records.

[*Back to Index*](#index)

## Article 35(9) – Consultation

* **Consultation process with data subjects & others**

*Was it undertaken? Do we need to? Do we need to get advice from experts?**Is their written advice already out there about this  
(NDG, GMC, MDU, BMA, UKCGC)?*

*Consultation with data subjects*

When considering whether consultation with patients was *necessary*, I took into consideration the following:

That the consumer organisations *already* had access to the GP record (via multiple routes). It would not be a “new thing” for either SCAS NHS 111 or NHUC (GP out-of-hours services) to have such access. All that would change would be the technical solution to achieve this and, as will be seen later, that migration to GP Connect ensured far better privacy, data protection, and data control by both the surgery and the patient (data subject).

That some patients have opted out of the National Summary Care Record and/or CHIE (our current LHCR). However, both those projects involve the wholesale *extraction and uploading* of GP record information into a third party database; in the case of the SCR, into the hands of a new data controller, in the case of CHIE, into the hands of a data processor under our instruction.

That (and see later for this) GP Connect will *de facto* become the single source of GP record information accessed by both SCAS NHS 111 and NHUC, and in due course SECAMB. In fact, it is likely that NHUC will have access *only* to GP Connect (though maybe still the SCR) in due course.

We have very few patients who have expressed a GP Connect “blocking” opt-out (93C1). Those historic objections have been from Monteagle Surgery patients and will have been coded as such to prohibit either CHIE, or risk stratification for case finding, or both. Such objections could (and should) be converted to 9Nd1+9q7 read code objections – so upholding their existing opt-outs whilst at least permitting the possibility of access via GP Connect (and indeed, access by Phyllis Tuckwell Hospice Care) with “permission to view”. The very fact that permission to view is strictly enforced in GP Connect significantly mitigates against any data protections concerns with such a conversion.

Accordingly, whilst ensuring a comprehensive fair processing campaign to inform our patients about GP Connect, and because of the strict explicit permission requirement to access GP Records via GP Connect, I do not think it necessary to consult with patients prior to the practice deciding on such processing.

*Consultation with others*From the beginning – when we were approached with the proposal of allowing access to GP records via GP Connect, I have been in close consultation with the BMA’s GPC IT Subcommittee.

I have sought advice on the exact process and safeguards involved in permitting a “GP Connect” link with an external, consumer organisation, directly from NHS Digital (Christopher Metzner, Implementation Manager, Implementation & Business Change – South).

Where necessary, I have sought advice and information, by email, more generally from NHS Digital enquiries.

I have been in contact with EMIS Health as regards the process, and safeguards, from our end as the “provider” organisation.

I have discussed GP Connect with NHUC (our GP OOH provider). It is clear that:

* NHUC are unhappy with CHIE  
  *“many comments from NHUC clinicians that CHIE is unreliable and not particularly user friendly so anything better would certainly have our vote”*
* Once NHUC migrate to the same Adastra database as SCAS (May), then GP Connect will be the single point of access for GP-held information
* This may well be voluntary, given their dissatisfaction with CHIE, but also because they are “*unlikely to be able to connect to more than the one external portal*” – so CHIE might well be switched off anyway

I have discussed GP Connect directly with SCAS NHS 111. It is clear that:

* SCAS NHS 111 are unhappy with CHIE – they find it temperamental as well, and far prefer a “real time” records view
* Where they are already using GP Connect, they absolutely love it
* They really, really want GP Connect for all NHS 111 calls (i.e. all practices)
* When available, it will be their single point of access for GP-held information. CHIE (and probably the SCR) will no longer be used.

I have discussed GP Connect directly with SECAMB:

* They would very much want access to GP Connect provided GP records
* They don’t have access to CHIE (nor seemingly, do they wish it)
* They already have partial access to GP Connect  
  *“HTML view and in-hours direct appointment booking (DAB) technical accreditation is completed for the 999 UI and middleware messaging”*
* *“GP Connect functionality is already built into our new ePCR system and, once accreditation is completed, will be accessible by all crews from their Trust iPads”*

It is therefore patently clear that NHUC, SCAS and SECAMB all want GP Connect, and will use it as their *single point* of GP records access once implemented.

I sought the advice of the Professional Records Standards Body, who recently produced their “Urgent care information flows” report:

<https://theprsb.org/wp-content/uploads/2018/11/IUC-information-requirements-final-report-LC-1.pdf>

In that report, they made mention of permission to view being a pre-requisite to information sharing:  
 *“4.4 Principles of information sharing  
 5. Consent should be noted for the person’s details to be shared with the next care provider”*

Any further comments from the PRSB are still awaited.

Frimley Park Hospital A&E (ED) have never used CHIE, don’t use CHIE, and are very unlikely ever to use CHIE. GP Connect would provide them with a straightforward, safe, consensual and transparent way for ED clinicians to access necessary and relevant information, when required, from the GP records of patients attending their department. There are no cost implications, and no approval is needed from any other organisation (other than OHG) to enable this (subject to their accreditation by NHS Digital).

[*Back to Index*](#index)

## Article 35(7)(b) - Necessity and Proportionality

* **Necessity and proportionality (data protection compliance)**

*“Principle 5*

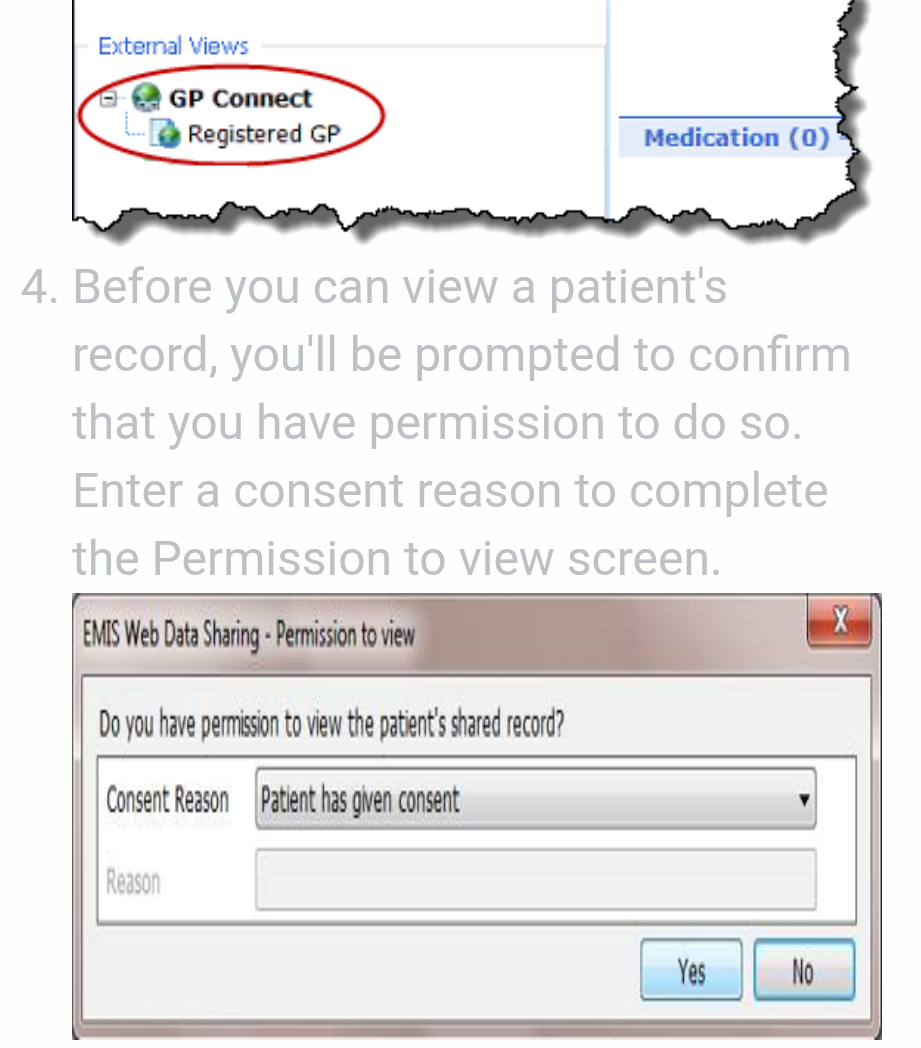
*Any arrangements agreed by NHS organisations should fully adhere to all applicable national level legal, regulatory, privacy and security obligations, including in respect of the National Data Guardian’s Data Security Standards, the General Data Protection Regulation (GDPR) and the Common Law Duty of Confidentiality.”*[DHSC, Creating the right framework to realise the benefits for patients and the NHS where data underpins innovation](https://www.gov.uk/government/publications/creating-the-right-framework-to-realise-the-benefits-of-health-data/creating-the-right-framework-to-realise-the-benefits-for-patients-and-the-nhs-where-data-underpins-innovation)

### Common Law (CLoC) *How is this met?*

Data protection law requires that personal data must be processed lawfully. This means it must be processed in accordance with any duty of confidentiality that applies. The ‘reasonable expectations’ of the patient should be the test as to whether a duty of confidence arises.

GP Connect fully complies with the common law of confidentiality. Whilst data is not extracted or uploaded *anywhere* outside of the GP surgery, but streamed in real time, EMIS mandates a strict “Permission to View” policy for GP Connect HTML Records access:

1. For GP surgeries viewing the records of another surgery (e.g. within a PCN)



1. And SCAS NHS 111 have a strict permission to view policy.  
   *“the GP Connect tab presents a permission to view qualifying question similar to Summary Care Record. Clinicians will seek permission and select Yes, No or Emergency. The response to this is recorded in the Event list of the case for historical reviewing/audit purposes.”*

There are no secondary uses of GP Connect derived data, so compliance with the CLoC for such purposes is not applicable.

* We rely on **implied consent** to make an individual’s GP record *accessible* via GP Connect.
* We rely on **explicit consent (permission)** to permit *access* to the personal confidential data, by the consumer organisation.

[*Back to Index*](#index)

### Caldicott Principles

*1. Justify the purpose(s)  
How is this met?*

The *sole* purpose is direct medical care.

*2. Don’t use personal confidential data unless it is absolutely necessary  
How is this met?*

Personal confidential medical data is necessarily required.

*3. Use the minimum necessary personal confidential data  
How is this met?*The information provided is limited to that which would be helpful to an out of hours service such as SCAS NHS 111, NHUC and SECAMB.

*4. Access to personal confidential data should be on a strict need-to-know basis  
How is this met?*

Only organisations who have a DSA in force, and agreed by NHS Digital, between the surgery and the organisation, can view records via GP Connect.

Within SCAS NHS 111, call handlers do NOT access medical records. Only if the call is escalated to a clinician (doctor/nurse/paramedic etc) within NHS 111 is the GP record accessed.

*5. Everyone with access to personal confidential data should be aware of their responsibilities  
How is this met?*

Consumer organisations must meet stringent accreditation with NHS Digital before access via GP Connect is permitted, including compliance with data protection principles.

*6. Comply with the law  
How is this met?*

Access to GP records, via accredited consumer organisations, and with the strict upholding of “permission to view” clearly complies with the law.

*7. The duty to share information can be as important as the duty to protect patient confidentiality  
How is this met?*The *ability* to share records via GP Connect – with the patient’s explicit permission – is enabled.[*Back to Index*](#index)

### Article 5 GDPR – the data protection principles

The fundamental principles which aim to ensure compliance with the spirit of data protection law and the protection of the rights of individuals (data subjects).

*Personal data shall be:*

*a) processed lawfully, fairly and in a transparent manner in relation to individuals (lawful purpose)*

* *A legal basis under GDPR*
* *Be otherwise compliant with the requirements of the GDPR and DPA 2018*
* *Not involve any otherwise unlawful processing or use of personal data*
* *Be fair towards the individual*
* *Avoid being unduly detrimental, unexpected, misleading or deceptive*
* *Clear and transparent to individuals and regulators*
* *Is this met?*

Yes. The legal bases for providing access to GP records in this way are

* Article 6(1)(e) – Official authority
* Article 9(2)(h) – Provision of Health

The Common Law of Confidentiality is upheld by means of permission to view (explicit permission to access the confidential data).

Processing is fair – not only can patients object to accessing their data contemporaneously (PTV) but can opt-out completely at the GP surgery.

*b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes  
(purpose limitation)*

* *Specified, explicit, legitimate purposes*
* *Clear and open from the outset*
* *Purposes in line with individual’s reasonable expectations*
* *How is this met? How do we prevent function creep?*

Processing is limited to direct care purposes only.  
Patients expect and want their medical information to be *available* to those within the NHS providing them with direct medical care, though they expect both to be asked first, and have the right to object.

It is reasonable that the out-of-hours “urgent” services would and should have this ability.

*c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (data minimisation)*

*“Necessary”:*

* *It must be a targeted and proportionate way of achieving that purpose*
* *It must be more than just useful or habitual*
* *We cannot reasonably achieve the same purpose by some other less intrusive means – and in particular if we could do so by using non-special category data*
* *It is not enough to argue that processing is necessary because it is part of our particular business model, processes or procedures, or because it is standard practice*
* *Organisations must comply with the minimisation principle under data protection law if using personal data. This means ensuring that any personal data is adequate, relevant and limited to what is necessary for the purposes for which it is processed*

*How is this met?*

GP Connect is a proportionate way of providing access to GP Records, without any data being uploaded to a 3rd party database.

Whilst SCAS NHS 111 does have access to similar data via CHIE, it is clear that they would far prefer to use GP Connect *instead* of CHIE, and it may well be that NHUC will be able to only use GP Connect. In time, SCAS may well disconnect from CHIE. In addition, GP Connect is likely to be the *only* way for SECAMB to access GP records information of this detail.

*d) accurate and, where necessary, kept up to date (accuracy)  
How is this met?*

The GP records are kept up to date. GP Connect provides a “real-time view” of the record to SCAS NHS 111.

*e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed (storage limitation)  
How is this met?*

No data is stored by the consumer organisation.

*f) processed in a manner that ensures appropriate security of the personal data (confidentiality)  
How is this met?*

No data is extracted or uploaded out of the GP records database.

[*Back to Index*](#index)

## No surprises

*“The Review Panel concluded that consent should be obtained before sharing a patient’s whole care record with other registered and regulated health and social care professionals for the purposes of direct care. Any exceptions to this guidance should be based on professional judgement in individual cases.”  
(*[*NDG, 2013 To share or not to share? The Information Governance Review*](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/192572/2900774_InfoGovernance_accv2.pdf)*)*

*“3.2.6 The Review heard that patients may have elements of their record that they do not want to be shared and felt that sharing their whole record was not necessary for direct care. In line with the Caldicott principles and the last review, only relevant information about a patient should be shared between health professionals in support of their care.  
Explicit consent should be obtained before accessing someone’s whole record."  
“3.2.0 …there should be ‘no surprises’ for the individual about who has had access to information about them.”  
(*[*NDG, 2016 Review of Data Security, Consent and Opt-Outs*](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/535024/data-security-review.PDF)*)**“…there must be no surprises to the citizen about how their health and care data is being used”  
“ Failing to offer this choice to people can accelerate discontent with how they are being informed and consulted, resulting in a growing rejection of the benefits of data sharing. “  
(*[*NDG*](https://www.gov.uk/government/speeches/national-data-building-trust-across-health-and-social-care)*,* *Building trust in the use of data across health and social care)*

*“You are quite correct in stating in your correspondence with my office that my 2016 and 2013 reviews re-iterated the Caldicott Principles, and that only relevant information about a patient should be shared between health professionals in support of their care. Both took the position that explicit consent should be obtained before accessing someone’s whole record.”  
(NDG, personal correspondence with Dr Neil Bhatia)*

*“29 If you suspect a patient would be surprised to learn about how you are accessing or disclosing their personal information, you should ask for explicit consent unless it is not practicable to do so (see paragraph 14). For example, a patient may not expect you to have access to information from another healthcare provider or agency on a shared record.”  
(*[*GMC*](https://www.gmc-uk.org/-/media/documents/confidentiality-good-practice-in-handling-patient-information---english-0417_pdf-70080105.pdf)*)*

*“If patients decide to have a shared record, their explicit consent to view must be obtained e.g. where a practice other than the patient’s registered practice is seeking to view the record for the delivery of out-of-hours care.  
In exceptional circumstances, for example if the patient is unconscious and immediate access to the record is necessary, it may be appropriate to access the record without consent to view.”  
(*[*BMA*](https://www.bma.org.uk/advice/employment/ethics/confidentiality-and-health-records/principles-for-sharing-electronic-patient-records)*)*

*“You have the right to be informed about how your information is used.  
You have the right to request that your confidential information is not used beyond your own care and treatment and to have your objections considered, and where your wishes cannot be followed, to be told the reasons including the legal basis.  
The NHS also pledges:* *where identifiable information has to be used, to give you the chance to object wherever possible.  
All staff have responsibilities to the public, their patients and colleagues. You should aim to: inform patients about the use of their confidential information and to record their objections, consent or dissent.”  
(*[*NHS Constitution, Respect, consent and confidentiality*](https://www.gov.uk/government/publications/the-nhs-constitution-for-england/the-nhs-constitution-for-england#patients-and-the-public-your-rights-and-the-nhs-pledges-to-you)*)*

*Is this met?  
Does the data subject know that we are disclosing?*

GP Connect fully upholds the “No surprises” principle.

Patients are asked for their “permission to view” before any such access takes place (except for a “break glass” emergency when the patient cannot consent).

GP Connect HTML records access meets the requirements and principles of the NDG, the GMC, the BMA and the NHS Constitution.

[*Back to Index*](#index)

## GMC Confidentiality Principles

***A Use the minimum necessary personal information.*** *Use anonymised*

*information if it is practicable to do so and if it will serve the purpose.*

***b Manage and protect information.*** *Make sure any personal*

*information you hold or control is effectively protected at all times*

*against improper access, disclosure or loss.*

***c Be aware of your responsibilities.*** *Develop and maintain an*

*understanding of information governance that is appropriate to*

*your role.*

***d Comply with the law.*** *Be satisfied that you are handling personal*

*information lawfully.*

***e Share relevant information for direct care*** *in line with the*

*principles in this guidance unless the patient has objected.*

***f Ask for explicit consent*** *to disclose identifiable information about*

*patients for purposes other than their care or local clinical audit,*

*unless the disclosure is required by law or can be justified in the*

*public interest.*

***g Tell patients*** *about disclosures of personal information you make*

*that they would not reasonably expect, or check they have received*

*information about such disclosures, unless that is not practicable*

*or would undermine the purpose of the disclosure. Keep a record of*

*your decisions to disclose, or not to disclose, information.*

***h Support patients to access their information.*** *Respect, and help*

*patients exercise, their legal rights to be informed about how their*

*information will be used and to have access to, or copies of, their*

*health records.*<https://www.gmc-uk.org/ethical-guidance/ethical-guidance-for-doctors/confidentiality/the-main-principles-of-this-guidance>

*Are these all met?*

Yes.

## The Human Rights Act 1998

Article 8 of the Human Rights Act protects our privacy, our family life, our home and our communications.  
*“Everyone has the right to respect for his private and family life, his home and his correspondence* “  
  
*Article 8 of the European Convention on Human Rights: Right to respect for private and family life*

This means respect for private and confidential information, including the storing and sharing of data. And that very much includes medical information (which includes correspondence between the patient and their healthcare providers).

The Human Rights Act 1998 made the ECHR part of domestic law.

*164. Respecting the confidentiality of health data is a vital principle in the legal systems of all the Contracting Parties to the Convention. It is crucial not only to respect the privacy of a patient, but also to preserve his or her confidence in the medical profession and in the health services in general.*

*Without such protection, those in need of medical assistance may be deterred from revealing such information of a personal and intimate nature as may be necessary in order to receive appropriate treatment and, even, from seeking such assistance. They may thereby endanger their own health and, in the case of communicable diseases, that of the community.*

*The domestic law must therefore afford appropriate safeguards to prevent any such communication or disclosure of personal health data as may be inconsistent with the guarantees in Article 8 of the Convention (Z v. Finland, § 95; Mockutė v. Lithuania, §§ 93-94).*

[*https://www.echr.coe.int/documents/guide\_art\_8\_eng.pdf*](https://www.echr.coe.int/documents/guide_art_8_eng.pdf) *Guide on Article 8 of the European Convention on Human Rights, Dec 2018*

GP Connect records access fully upholds Article 8 of the HRA. Patients are asked for their explicit permission *before* any information from their GP record is accessed in this way.

In doing so, patients can say “no” – and no such information will be accessed.

In an emergency, when the patient does not have the capacity to consent, and assuming the patient has not opted out completely of GP Connect (93C1 objection), access to the GP record without is still permissible under vital interests/public interest (“so called “break glass” emergency access).

[*Back to Index*](#index)

## Data Processors – Article 28

*A controller determines the purposes and means of processing personal data.  
A processor is responsible for processing personal data on behalf of the controller and can act only upon the instructions of the controller.  
Does the practice retain full data controllership?  
How do we ensure that processors comply?*

*Does processing require the use of a data processor?*  
**NO**

*If yes:*

Has a **written** data processor contract been provided?  
**Choose an item.**

Are both the controller and processor **parties** to the contract?  
**Choose an item.**

Are both controller and processor **signatories** to the contract?  
**Choose an item.**

*Does the processor contract contain the following compulsory details?*

* the name of the controller and the processor  
  **Choose an item.**
* contact details for the controller and the processor  
  **Choose an item.**
* the subject matter and duration of the processing  
  **Choose an item.**
* the nature and purpose of the processing  
  **Choose an item.**
* the type of personal data and categories of data subject  
  **Choose an item.**
* the obligations and rights of the controller  
  **Choose an item.**

*Does the processor contract contain the following compulsory terms?*

* the processor must only act on the written instructions of the controller (unless required by law to act without such instructions)  
  **Choose an item.**
* the processor must ensure that people processing the data are subject to a duty of confidence  
  **Choose an item.**
* the processor must take appropriate measures to ensure the security of processing  
  **Choose an item.**
* the processor must only engage a sub-processor with the prior consent of the data controller and a written contract  
  **Choose an item.**
* the processor must assist the data controller in providing subject access and allowing data subjects to exercise their rights under the GDPR  
  **Choose an item.**
* the processor must assist the data controller in meeting its GDPR obligations in relation to the security of processing, the notification of personal data breaches and data protection impact assessments  
  **Choose an item.**
* the processor must delete or return all personal data to the controller as requested at the end of the contract  
  **Choose an item.**
* the processor must submit to audits and inspections, provide the controller with whatever information it needs to ensure that they are both meeting their Article 28 obligations, and tell the controller immediately if it is asked to do something infringing the GDPR or other data protection law of the EU or a member state  
  **Choose an item.**

*Does the processor contract?*

* state that nothing within the contract relieves the processor of its own direct responsibilities and liabilities under the GDPR  
  **Choose an item.**
* reflect any indemnity that has been agreed  
  **Choose an item.**
* contain an expiration date for processing (after which all processing must cease)  
  **Choose an item.**
* Make clear how either the data controller or the data processor may voluntarily terminate the contract, including the notice required  
  **Choose an item.**

*Is it clear that the data processor must?*

* only act on the written instructions of the controller (Article 29)  
  **Choose an item.**
* not use a sub-processor without the prior written authorisation of the controller (Article 28.2)  
  **Choose an item.**
* co-operate with supervisory authorities (such as the ICO) in accordance with Article 31  
  **Choose an item.**
* ensure the security of its processing in accordance with Article 32  
  **Choose an item.**
* keep records of its processing activities in accordance with Article 30.2  
  **Choose an item.**
* notify any personal data breaches to the controller in accordance with Article 33  
  **Choose an item.**
* employ a data protection officer if required in accordance with Article 37  
  **Choose an item.**

*Does Oakley Health Group retain* ***full data controllership*** *over all aspects of processing?*  
**Choose an item.**

*Is Oakley Health Group inadvertently becoming a data controller for information out with the GP record?***Choose an item.**

Whilst a data *processor* contract is not needed, a data sharing agreement (DSA) between the provider (OHG) and the consumer (SCAS NHS 111) organisations is required before NHS Digital will approve and enable such access. We have been provided with a DSA.

There are unnecessary references to “direct appointment booking” within the DSA. Direct appointment booking, whilst enabled by GP Connect, is quite separate from records access and does not involve the disclosure of personal data, by OHG, in any way.

That aside, the DSA is a bog-standard agreement between two controllers, and whilst not a legal obligation, it is good practice, and a contractual obligation anyway for NHS Digital to enable the link.

[*Back to Index*](#index)

## Article 25 (2) – Data Protection by Default

*Data Protection by design and default is* ***a legal requirement under GDPR.****Article 25 specifies that, as the controller****, we have responsibility*** *for complying with data protection by design and by default  
  
‘The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.’**Are we “not processing additional data unless the individual decides we can”?  
Are we “providing individuals with sufficient controls and options to exercise their rights”?* Considerable effort has gone into the design of GP Connect to ensure data protection by default. A data sharing agreement is compulsory, NHS Digital must approve any such link once an accreditation process by the consumer has been completed. Data is provided in a read-only, real-time, “streaming” way, with no data being extracted and uploaded to a 3rd party database. No secondary uses of the shared data are permitted (or possible). A strict “permission to view” policy is in force. Patients are therefore informed and offered the opportunity to object each time they contact SCAS NHS 111 (or any subsequent consumer organisations).  
[*Back to Index*](#index)

### Data Processors (Article 28)

*Are we only using a data processor that provides “sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject”?*

N/A

[*Back to Index*](#index)

### Privacy as the default setting

*Is it?*Yes. No data is extracted or uploaded out of the GP records database. No data is viewable without the patient’s explicit permission.

[*Back to Index*](#index)

### Privacy embedded into design

*Is it?*

Yes.

[*Back to Index*](#index)

## Ability to implement Data Subject Rights

*How is this met?*

1. ***The Right to be informed****Can we provide a comprehensive privacy policy?  
   How are people informed about this use of their data?  
   Can we provide an appropriate one for children if needs be?  
   Is another data sharing project being launched at the same time?*

Providing a straightforward privacy policy (and a factsheet) will be easily achievable. We will need to advertise this new route to records access via the usual means (poster, leaflets, website, Facebook etc).  
Very importantly, the right to be informed is also upheld *each and every time* that permission to view is sought by SCAS NHS 111.

1. ***The Right of access***  
   *If a processor is used, how does the subject access the data held by the processor?*  
     
   N/A. The right of access lies with the GP record.
2. ***The Right to rectification****If a processor is used, does this extend to the data held by the processor?  
   Or is that data simply a reflection of the data held in the GP record (with its own obligation to rectification)?*  
     
   N/A. The right of rectification lies with the GP record.
3. ***The Right to object****Where does processing take place? Extraction/Uploading/Disclosure/Access?  
   Where does any objection or opt-out act?  
   Is there a granular objection/opt-out mechanism?*GP Connect fully upholds the right to object.  
   Permission to View affords the data subject the contemporaneous opportunity to object to any specific access situation.  
   Patients can express a permanent objection (“opt-out”) via the GP surgery that will prohibit records sharing via GP Connect, even in an emergency “break glass” situation.

However, that objection (93C1) has additional effects, also opting the patient out of EMIS Web data sharing of the GP record with Phyllis Tuckwell Hospice, CHIE, and risk stratification for case finding.  
Opting out of CHIE, or continuing to uphold any such objection, is achievable by means of the 9Nd1 read code flag (which will then not prohibit GP Connect).

Opting out of risk stratification for case finding (a secondary use processing, authorised by s251 HRA/CAG approval), or continuing to uphold any such objection, is achievable by means of either the 9q7 or the 9Nu0 (Type 1 opt-out) read code flag (which will then not prohibit GP Connect).[*Back to Index*](#index)

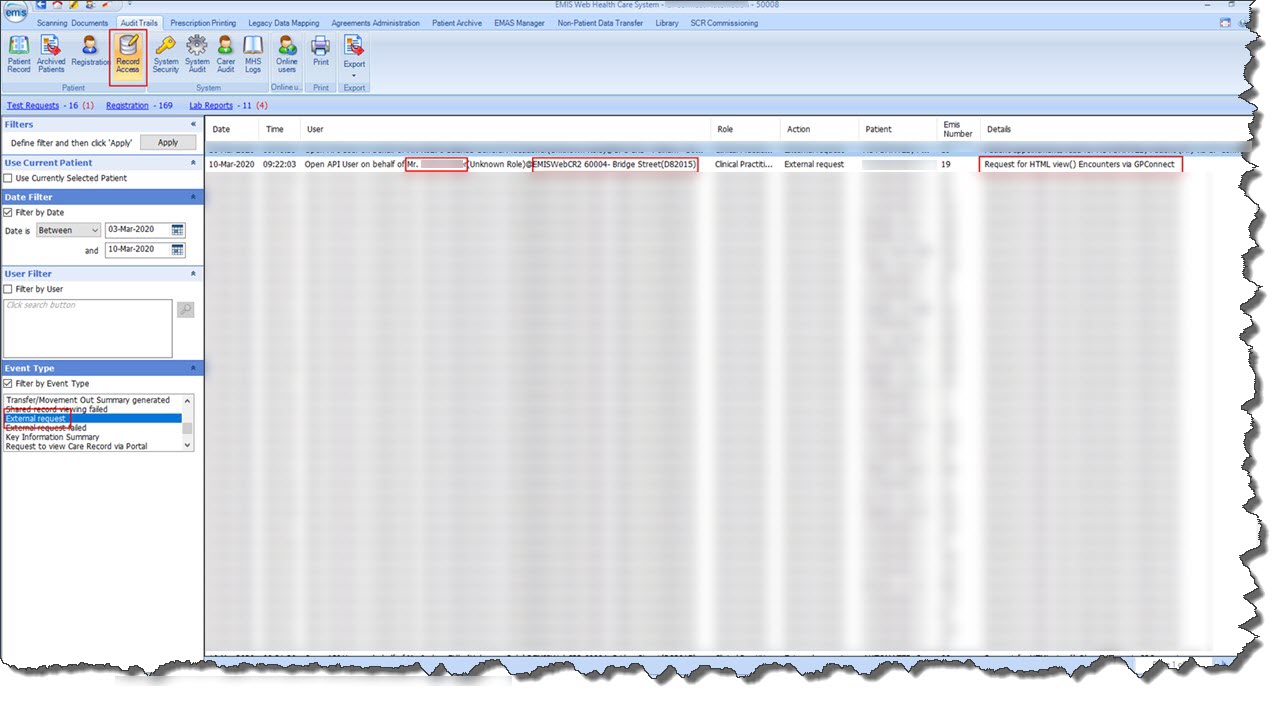
## Things to think about

### Surrender of control

*A disclosure to another data controller = a surrender of control*The GP surgery retains *full* control of the processing. There is no disclosure of information, but *access to* information.

We can turn such access on and off, as we see fit, directly within our EMIS Web system.

We can audit any access of a patient’s record undertaken via GP Connect (via **Audit Trails > Record Access > Event type = External request).** The organisation and user which the request came from is (usually) within the 'User' column.



### Do we have to do disclose?

*What legislation mandates this? Is this just a contractual obligation?*

No, we do not have to enable GP Connect. It is neither a legal nor a GMS contractual requirement.

[*Back to Index*](#index)

### Can we do this without processing the data? Can we do this, or process data, in a less intrusive way?

*Is there a better way? Is this necessary (the most appropriate choice)?*

Arguably, SCAS NHS 111 already have access to equivalent information via CHIE.  
  
However, it is clear that SCAS sees GP Connect as the future, single source of GP records information. And for NHUC, once using the same Adastra database as SCAS, GP Connect might be the *only* way of accessing such a level of information.

GP Connect is *less intrusive* than either the SCR or CHIE – no data is extracted or uploaded to a 3rd party database (both SCR and CHIE), and no secondary processing is permitted (CHIE).

Whilst the SCR fully respects permission to view, there is an increasing move within CHIE towards a *complete withdrawal* of permission to view. This will raise serious data protection issues.[*Back to Index*](#index)

### Is this lawful?

* ***Common law, and***
* ***Caldicott Principle 6, and***
* ***Article 5(a) GDPR, and***
* ***Any other relevant laws (e.g. PECR, Article 10 GDPR)***

Yes, this is lawful.[*Back to Index*](#index)

### Is this ethical? Is this fair?

*“You need to stop and think not just about how you can use personal data, but also about* ***whether you should****” (ICO)*

Yes, this is ethical.

*Fairness*

It could be argued that the introduction of yet another data sharing scheme, on top of the SCR and CHIE, is unfair, given that patients who had already objected to, or opted out from, the SCR and CHIE will find that their GP records are accessible in this way. GP Connect does not recognise either the SCR opt-out (9Ndo) or the CHIE opt-out as recorded by OHG (9Nd1).

In mitigation, however:

* any access via GP Connect is under a strict permission to view policy
* many patients who had previously opted out of the SCR and/or CHIE did so because of:
  + concerns over the extraction and uploading of personal data to a 3rd party database (and in the case of the SCR, a different data controller)
  + concerns over secondary uses of personal data for undefined secondary purposes and the transfer of personal data to a further database (CHIA) under the control of a different data controller (in the case of CHIE)

GP Connect neither uploads data to a new database, nor permits any secondary uses of viewed data.

[*Back to Index*](#index)

### Is there a risk of reputational damage if we proceed with processing?

*To the practice/To the profession/What would the GMC say?  
What would our patients think?*

Maintaining trust in doctors, and general practice, is vital if we are to continue the level of doctor-patient relationship that facilitates disclosure of sensitive, personal, confidential information from an individual seeking health care to their healthcare professional.

*“So, yes, the world is changing, the health landscape is changing, patients are changing, but amongst all of this is one constant – our trust in our doctors.”*Trust: the Truth?<https://www.ipsos.com/sites/default/files/ct/publication/documents/2019-09/ipsos-thinks-trust-the-truth.pdf>

*“The protection of personal data, not least medical data, is of fundamental importance to a person’s enjoyment of his or her right to respect for private and family life as guaranteed by Article 8 of the Convention (art. 8). Respecting the confidentiality of health data is a vital principle in the legal systems of all the Contracting Parties to the Convention. It is crucial not only to respect the sense of privacy of a patient but also to preserve his or her confidence in the medical profession and in the health services in general.*

*Without such protection, those in need of medical assistance may be deterred from revealing such information of a personal and intimate nature as may be necessary in order to receive appropriate treatment and, even, from seeking such assistance, thereby endangering their own health and, in the case of transmissible diseases, that of the community”*Z v. FINLAND - 22009/93 - Chamber Judgment [1997] ECHR 10 (25 February 1997)

<https://www.bailii.org/eu/cases/ECHR/1997/10.html>  
  
Our patients expect to make available necessary and relevant data within the NHS, as long as such access (or disclosure) is lawful, fair, consented, proportionate, transparent, informed, and where patients can exert genuine control over such sharing of their personal data.

GP Connect meets all of these criteria, by virtue of a read-only, “streaming”, records access API, by a strict “permission to view” policy, and by ensuring that the practice retains full control of the processing.

[*Back to Index*](#index)

### What are the consequences of not proceeding with this processing? Can we mitigate against any negative effects?

*Does it matter at all if we say no?*

For a while anyway, both SCAS NHS 111 and NHUC will continue to have access to GP records via the SCR, CHIE, and bespoke data sharing mechanisms such as Adastra Special Patient Notes (SPN).

But very soon, it may well be that NHUC can access GP records *only* via GP Connect, and SCAS will want to access GP records *only* via GP connect (or indeed, may switch off CHIE completely).

SECAMB (our ambulance service) has no access to CHIE, and the provision of GP records access via GP Connect may afford them the only route.

[*Back to Index*](#index)

### What about children?

*A child’s personal data merits particular protection under the GDPR.  
Fairness, and compliance with the data protection principles, should be central to all your processing of children’s personal data.  
If you profile children then you must provide them with clear information about what you are doing with their personal data.  
You must write clear and age-appropriate privacy notices for children.*

We will need to update our privacy policies to make clear this route, addition in the first instance, of records access by organisations involved in the delivery of out-of-hours (and in hours) care.

[*Back to Index*](#index)

### How does this compare with other, similar data sharing projects?

*Are there similar data sharing projects already in existence, even locally?  
How does data protection in those projects compare with this project?*  
Yes. The SCR and CHIE are similar data sharing projects. See [Conclusion](#conclusion) for the comparison.

[*Back to Index*](#index)

## Article 35(7)(c)

* **Risks to data subjects**

*What are they?   
Function creep?  
Breach of privacy/confidentiality?  
Inability to control data?*GP Connect fully upholds the right to be informed and the right to object.

Permission to View upholds these, as well as ensuring compliance with the CLoC, GMC and BMA guidance on shared records, as well as the NDG’s “no surprises” principle.

Function creep is not an issue, as no data is handed over to another organisation (so no secondary uses, or “re-purposing” is possible).

Individual data sharing agreements, and NHS Digital accreditation requirements, ensure that organisations who *can* access GP records information via GP Connect are strictly controlled, and require prior authorisation from the surgery.

Because of Permission to View, there would not be a breach of privacy. Article 8 of the HRA is fully upheld. Nothing is disclosed or accessible without the patient’s say so.

Except in a “break glass”, emergency, scenario, there will not be a situation where a patient discovers that their personal confidential medical information, as held by their GP, has been accessed by someone out with their GP surgery *after* such access has happened.

There will be “no surprises”.

The same cannot be said for some LCHRs (notably Connected Care, but also – potentially – CHIE).

Patients can control data on a case by case basis – perhaps allowing access when systemically unwell but not allowing access for minor injuries or enquiries.

Patients can also opt-out completely of GP Connect records sharing.

The amount of information available to SCAS NHS 111 is fairly detailed. In mitigation, the NHS 111 call handlers do **not** access the GP record, it is only the clinicians that do once the call has been escalated to them

[*Back to Index*](#index)

## Article 35(7)(d)

* **Measures to manage, reduce or eliminate risks**

*What can we do?  
What safeguards or measures would mitigate the risks?*

Permission to View mitigates against any risks such as the patient not being informed or afforded the opportunity to object.

Whilst it might, at face value, appear unfair to “enable” another route to GP records, by an external organisation, for those patients who had, in good faith, opted-out of the SCR and CHIE, permission to view and the fact that no data is transferred from the GP records database provides strong safeguards and mitigates the risk of “unfairness”.

Individual data sharing agreements, and NHS Digital accreditation requirements, ensure that organisations who *can* access GP records information via GP Connect are strictly controlled, and require prior authorisation from the surgery.

Good privacy notices, and a widespread information programme, will demonstrate transparency and a willingness to try to ensure that patients understand the new access, and the benefits that it brings to the consumer organisations.

[*Back to Index*](#index)

## Conclusion

* **Article 36 – Need for prior consultation with the ICO**

*Do we need to?*

No, we do not need to consult with the ICO prior to making any decision on processing.

*Can we disclose, and do we want to disclose?*

GP Connect provides a safe, transparent, consensual, and proportionate way of making relevant and necessary information from the GP record available to organisations currently providing our patients with   
out-of-hours, some in-hours, and emergency, care : SCAS NHS 111, NHUC (our GP out-of-hours provider), and SECAMB. And, perhaps in time, the ED at Frimley Park Hospital.

The strict adoption of “Permission to View” (PTV) ensures compliance with the CLoC, GMC and BMA guidelines on shared record access, and the principles expressed by the NDG. It ensures that we uphold the data subject’s right to be informed, the right to object, and the right not to be surprised by how their personal confidential data is being used.

Where medical information has *already* been provided to an organisation, PTV mitigates against the disclosure of unnecessary – and therefore *excessive* – information.

Permission to View is a crucial component of NHS England’s Integrated Urgent Care Service Specification – and so GP Connect fully complies with that.  
  
*“5.13.3. Permission to View (PTV)*

*In situations where the patient may call one organisation then be passed to others, as part of receiving care, any information provided to patients must explain this. This includes capturing permission to view (PTV) of any records. The information provided on the original call must provide a clear and succinct explanation that sets the clear expectations for the patient on how their information will be accessed and used. When closing a call, a summary of what will happen next should include any information that will be provided.”*  
<https://www.england.nhs.uk/wp-content/uploads/2014/06/Integrated-Urgent-Care-Service-Specification.pdf>

And indeed, organisations tendering for such services are including that explicit requirement. For example:  
  
*“The Provider will ensure that all staff are trained and understand the importance of information governance, including the requirement for patients to give express permission to view records (PTV) unless a duty of care circumstance arises….”*  
[Integrated Urgent Care Service Specification for East Surrey CCG, Guildford & Waverley CCG, North West Surrey CCG, and Surrey Downs CCG](https://www.nwsurreyccg.nhs.uk/stay-informed/documents/nhs-111-1/406-specification-version-2/file)

It should be noted that The National Summary Care Record has a strict [PTV policy](https://digital.nhs.uk/binaries/content/assets/website-assets/services/summary-care-record/scr-permission-to-view-guidelines.pdf).

However, as regards CHIE:

* Currently, the policy remains ambiguous and open to interpretation

*“Data accessed under this agreement is subject to explicit consent from the Data Subject where this is practical. If a health care professional requires access to a data subject’s record and they were unable to obtain consent, they must only access the record where it is of clinical benefit to the patient to do so. This may apply in cases where a data subject is not present or unresponsive or access to their record is required in order to prepare for a consultation with that data subject.“  
“Where practical users should ask the patient before accessing CHIE. If the patient is unconscious or not present but would benefit from use of CHIE, users should exercise their professional judgement.”*

* It *might* be that – similar to [Connected Care](https://www.dropbox.com/s/7g254fe4mui70lm/OHG%20SYC%20DPIA.docx?dl=0) (a neighbouring LHCR, also “managed” by SCW CSU) – CHIE moves to a complete withdrawal of PTV. That move will, no doubt, occur without any consultation with data controllers or data subjects.

A complete withdrawal of PTV would raise serious data protection issues and would pose serious problems were the CSU to seek practices to sign such a revised data processor contract. Especially if, as appears to be the case, an assertion is *also* made that the CCG is – *somehow­* - the “lead data controller” for the GP data that the practice uploads to the data processor.

A “core” Summary Care Record, which the overwhelming majority of patients (who have not opted out) have, contains little useful information however – allergies and medication only. In contrast with CHIE, there are **no** secondary uses of data uploaded to the National Summary Care Record.

Whilst relatively detailed information is available to NHS 111, it is only the clinicians working there that will access the GP record, and then only if the call is escalated to them. And then again, only with permission to view.

It is my conclusion that GP Connect provides a safer, simpler, richer, more transparent, more reliable, and clearly consented (PTV) route to GP records access than either the SCR or CHIE.

It is eagerly sought by SCAS, NHUC and SECAMB, in preference to the SCR and CHIE. It might be the *only* route of access to GP records for NHUC and SECAMB, and certainly would be the chosen single route for SCAS.

Those organisations very much want us to provide them with access via GP Connect.

The number of patients for whom a GP Connect derived record would be accessible is far in excess of those having a SCR or CHIE record. This is principally because very few patients have expressed a 93C1 objection, but many have expressed a SCR (9Ndo) and/or CHIE (9Nd1) objection.

In contrast to CHIE, no data is uploaded, there are no secondary uses, and permission to view is strictly upheld and a *permanent* information governance feature.

GP Connect provides OHG with ultimate control over such processing – the ability to turn access off at will, and a comprehensive audit feature built in to EMIS Web.

The adoption of GP Connect raises the very real possibility that CHIE will, in time, no longer be used by *any* of the out-of-hours organisations; such processing (access) then might be viewed as unnecessary (by those organisations) and compete withdrawal from CHIE would be the logical and “data compliant” next step for them.

And indeed, possibly for OHG, especially as profoundly detrimental (and IMO, unlawful) changes to access governance might be on the cards, and a revised and unacceptable data processor contract – attempting to devolve or shift data controllership from the surgery to the CCG - might be attempted. As it is, our *current* data processor contract for CHIE does not meet [the requirements of Article 28](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/contracts-and-liabilities-between-controllers-and-processors-multi/what-needs-to-be-included-in-the-contract/), let alone any revised one in the pipeline.

The knowledge that saying to “No” to either or both of these changes, or to an inadequate and non-complaint contract, would not impact on the ability of SCAS/NHUC/SECAMB to access GP records (via GP Connect) will be of considerable benefit and reassurance.

We will need to ensure a comprehensive campaign to inform our patients of any such new processing, and of their right to opt-out. They must be afforded the opportunity to opt-out *before* such access is turned only. My suggestion would be for a (maximum) 2 week publicity programme, with the intention of turning on GP Connect records as soon as is reasonable given the current demands placed upon NHS 111.

We should not promote, encourage, or endorse data sharing methods that disregard permission to view and that both threaten data subject rights and ignore sound governance advice from reputable organisations such as the NDG, the GMC, and the BMA.

LHCRs, in particular, that ignore, or plan to ignore, permission to view are (in my opinion) archaic and profoundly paternalistic in their approach to the data subjects that they purport to serve.

We can, and in my opinion *should*, endorse and promote *any* data sharing project that upholds such data subject rights, ensures permission to view, and ensures full control by GP surgeries, as a sound replacement for the LHCRs that disregard those fundamental principles.

[*Back to Index*](#index)

## Sign Off

This DPIA will:

* Be circulated to all GP partners at OHG to decide whether to proceed with such processing, in line with our DPIA policy
* In the event of agreement to proceed with this project, be published and available to patients, linked to within our privacy notice for this processing
* Therefore, be disclosable under FOI
* Therefore, be publicly available

Dr Neil Bhatia



GP, IG/FOI/Records Access lead, Caldicott Guardian, DPO

Oakley Health Group

Date:

## Appendix 1 – Attached Documents





