**Data Protection Impact Assessment**

**Interface Clinical Review Services**

**CKD Medicines Optimisation Review Service**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Document File Name**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Version Date 23.12.2022**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Practice Name The Scott Practice**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Address**

**Greenfield Lane, Balby, Doncaster, DN4 0TG**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Data Protection Officer Caroline Million**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Other Practice Staff consulted**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Signed off by R Fells, Managing Partner. Dr K Mansfield and Dr E Gomersall**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Date**

**\_\_\_\_\_\_\_\_\_\_23.12.2022\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Contents**

[**1.** **INTRODUCTION** 2](#_Toc14174652)

[**2.** **DESCRIPTION OF PROCESSING** 2](#_Toc14174653)

[**3.** **SCREENING ASSESSMENT** 3](#_Toc14174654)

[**4.** **DATA FLOWS** 3](#_Toc14174655)

[**5.** **LEGAL BASIS FOR ACCESSING PATIENT DATA** 5](#_Toc14174656)

[**6.** **TECHNICAL SECURITY MEASURES** 5](#_Toc14174657)

[**7.** **ORGANISATIONAL SECURITY MEASURES** 5](#_Toc14174658)

[**8.** **PATIENT CONFIDENTIALITY** 6](#_Toc14174659)

[**9.** **RISK ASSESSMENT** 7](#_Toc14174660)

# **INTRODUCTION**

* 1. The Information Commissioner’s Office endorses a “privacy by design” approach to ensure that new services consider privacy and data protection compliance from the start[[1]](#footnote-1).
	2. This data protection impact assessment has been produced to assess the privacy risks of the Practice working with a third party to support the direct care of patients.

# **DESCRIPTION OF PROCESSING**

* 1. The Practice has requested an independent third party, Interface Clinical Services Ltd (Interface), to carry out a clinical review service for them. Interface employs pharmacists to deliver clinical or therapy review services on behalf of the NHS, pharmaceutical industry, medical device or other healthcare companies.
	2. Interface services are designed to assist healthcare organisations implement systematic approaches to the health and wellbeing of patients with conditions such as asthma, atrial fibrillation, chronic obstructive pulmonary disease, diabetes or osteoporosis.
	3. Interface completes clinical projects in approximately 3,000 GP practices and hospitals around the UK over the course of a year.
	4. Interface is an NHS Business Partner and meets the same Information Governance requirements as NHS organisations including completion of the NHS Data Security and Protection Toolkit. Confirmation that the company has completed the toolkit can be found on the [NHS Digital](https://www.dsptoolkit.nhs.uk/OrganisationSearch?searchValue=interface) website.
	5. Interface is also registered with the Information Commissioner’s Office[[2]](#footnote-2), has a Senior Information Risk Owner, a Caldicott Guardian and a registered Data Protection Officer who monitors compliance with GDPR.
	6. The Practice will sign an Authorisation Form and Protocol that provide direction on the clinical conduct of the review and act as a data processing agreement between the Practice (Data Controller) and Interface (Data Processor).
	7. Interface will then be authorised by the Practice to access their clinical system, carry out searches and screen patients. Any recommendations authorised by a Practice GP will be implemented on the system and communicated to patients.

# **SCREENING ASSESSMENT**

* 1. These questions are intended to help decide whether a PIA is necessary. Answering ‘yes’ to any of these questions is an indication that a PIA must be carried out.

|  |  |
| --- | --- |
| Will the project involve the collection of additional information about individuals?Information about health status, risk, treatment recommendations and interventions authorised by GPs may be recorded in practice systems. | YES/~~NO~~ |
| Will the project compel individuals to provide information about themselves? | ~~YES~~/NO |
| Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?Health records will be available to Interface, as a third party, to support the direct care of patients.  | YES/~~NO~~ |
| Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used? | ~~YES~~/NO |
| Does the project involve you using new technology that might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition. | ~~YES~~/NO |
| Will the project result in you making decisions or taking action against individuals in ways that can have a significant impact on them?Information will be presented to the GP who will make the clinical decision | ~~YES~~/NO |
| Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example, health records, criminal records or other information that people would consider to be private.Health records | YES/~~NO~~ |
| Will the project require you to contact individuals in ways that they may find intrusive? | ~~YES~~/NO |

**OUTCOME - a full Privacy Impact Assessment is required**

# **DATA FLOWS**

**Practice-based review**

* 1. Interface pharmacists access and review data directly in the Practice clinical system using a user name and password provided by the organisation and their own NHS Smartcard. The searches are restricted to the data that is required to deliver a specific service.
	2. Pharmacists carry out a clinical review of patients and present GPs with a list of recommendations. This may include making a medicinal or non-medicinal intervention and / or inviting the patient into a clinic. Those interventions authorised by the GP will be actioned on the practice system and communicated to the patient by letter or telephone.
	3. Interface uses Docmail, a secure mail management service provided by an NHS Business Partner, for patient mailings with practice approval. Letters are sent on behalf of the practice using the practice letterhead.
	4. Pseudonymised[[3]](#footnote-3) data is uploaded securely to Interface’s database system for quality assurance and quality control purposes. The authorisation form also provides permission for Interface to create anonymous aggregated data for external reporting, research and publication. All data is fully anonymised after thirty days.
	5. Data will not be disclosed to third parties. However, for reviews that are sponsored by a pharmaceutical company, Interface pharmacists have legal and contractual obligations to report any safety information or pharmacovigilance events they detect when reviewing patient records. The only personal data is transferred to the pharmaceutical company is the patient initials, age, gender and safety information.

**Reviews with remote access**

* 1. For some reviews, a remote dial in may be carried out by Interface technicians in advance to extract and prepare data for use by the pharmacist team in practice or after an agreed period to report on outcomes.
	2. Interface technicians dial in remotely to practice computer systems directly through a secure encrypted HSCN connection or using an encrypted remote access tool.
	3. Patient identifiable data extracted by the remote searches is transferred securely to Interface systems for processing and then transferred securely back to the practice.
	4. For all services except the QOF service, the data is then immediately and permanently deleted. For the QOF service, Interface removes patient names from the data and retains it until the end of the year following the year in which the service was provided to allow for re-audit. The data is then permanently deleted.
	5. Spot checks and audits are carried out to ensure that data has been pseudonymised and anonymised correctly.
	6. Practices are again asked to provide a unique user name and password for the technician or authorise their NHS Smartcard to ensure they can audit Interface access to the practice system.
	7. Any member of staff who has been authorised to work from home will have signed a remote working agreement that sets out the additional safeguards required to ensure data remains confidential when working remotely and will be provided with a laptop that has been encrypted to NHS standards.

# **LEGAL BASIS FOR ACCESSING PATIENT DATA**

* 1. The Data Controller (GP practice) remains responsible for recording the legal basis for processing patient data. Interface then accesses patient data as a Data Processor under a signed contract with the Practice, the Data Controller.
	2. All reviews are authorised through an Authorisation Form and Protocol that the lead GP and practice manager sign to permit Interface to process data on their behalf and to specify the scope of clinical interventions. All individual patient interventions are also authorised by the lead GP.
	3. These documents form the written contract for data processing that is required for data protection purposes and give Interface contractual obligations to ensure security of all patient identifiable data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational security measures.

# **TECHNICAL SECURITY MEASURES**

* 1. A unique user name and password must be set up by the practice before practice systems are accessed and Interface staff are also provided with an NHS Smartcard.
	2. Interface internal systems are protected by a managed firewall, access controls, encryption and virus and malware protection.
	3. Interface meets the standards of the NHS Data Security & Protection Toolkit and has achieved Cyber Essentials Plus certification, a Government backed scheme that helps protect organisations against common cyber-attacks, which is verified by independent experts. Penetration testing has also been carried out by an independent cyber security company.

# **ORGANISATIONAL SECURITY MEASURES**

* 1. All Interface staff have a contractual obligation to maintain patient confidentiality. All staff who will access patient identifiable data and see patients have an enhanced criminal record check on appointment and every three years thereafter.
	2. All staff complete the NHS Data Security training on induction and annually thereafter. The company also follows the NHS requirements for reporting security events and incidents.
	3. All Interface staff complete a comprehensive training programme that covers information governance and confidentiality, training on NHS IT systems and on the clinical reviews.
	4. Staff must demonstrate their competence on all these aspects before being signed off to deliver services independently. Once signed off, staff are regularly field visited, which is a structured process designed to assess whether they are meeting all the required standards.
	5. With the agreement of the Practice, Interface may carry out a quality assurance audit for a percentage of reviews to check that the review has been delivered to the required standard.

# **PATIENT CONFIDENTIALITY**

* 1. Any patient that has asked the practice to restrict the viewing of their record is excluded from the review.
	2. Patients within England have the right to opt out of their personal confidential information being shared for purposes other than their own direct care. Opted-out patients are included in Interface reviews, as the reviews are for the direct care of the patient.
	3. Interface will apply the national data opt-out from March 2021, or as soon as the functionality to flag opted-in patients is released in practice systems, and will then ensure that information about opted-out patients is not used for secondary purposes.

# **TRANSPARENCY**

* 1. The Interface website contains a [privacy notice](https://www.interface-cs.co.uk/privacy-notice/) that describes all the data processing that Interface does including the work carried out on behalf of GP practices.
	2. Interface recommends that GP practices update their own privacy notices to reflect the use of third parties.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **RISK ASSESSMENT**This table describes the risks that the project will fail to comply with data protection legislation and the actions taken to reduce the risks.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **No.** | **Risk** |  **Solution(s)** | **Result:** is the risk eliminated, reduced, or accepted? | **Evaluation:** is the final impact on individuals justified, compliant and proportionate?  | **Approved by:**  |
| (1) | There is a risk that the legal basis for a third party to access patient data is challenged. | A written contract for data processing, as required by data protection legislation, is signed between the practice and Interface before any patient data is accessed. A copy of this contract is left with the practice and retained by Interface, as required by the Information Commissioner. | This risk is therefore eliminated. | There is a clear legal basis for third party access to the patient data and the required records will be in place before data is accessed. The final impact on individuals is therefore justified.  |  |
| (2) | There is a risk that patient confidentiality could be compromised should Interface staff not be fully aware of, trained and supported in information governance, data protection and confidentiality.  | Interface mitigates this risk through: * Maintaining NHS Business Partner status
* Meeting legal obligations, for example, for retaining records of data processing
* Staff employment contracts, criminal record checks and professional code of conducts
* Staff training on induction, during training and annually thereafter
* Designating appropriately experienced SIRO, Caldicott Guardian and Data Protection Officer
* Contractual commitments to data controllers in Authorisation Forms with daily compliance check
* Robust policies and procedures including incident reporting, audit and field visits
* Regular updates on key IG issues
* Culture of IG awareness
 | This risk is therefore significantly reduced and accepted. | Yes, Interface only accesses data that it has a legal basis for accessing and for purposes compatible with the purpose for which it was collected. Such data is only accessed by registered health care professionals or technicians who are comprehensively trained in information governance, have a criminal record check and are contractually committed to confidentiality.  |  |
| (3) | There is a risk that patients will object to the processing of data by a third party. The information Commissioner advocates the use of privacy or fair processing notices for transparency so that people are aware of how their data is used.  | The GP, as data controller, is responsible for reflecting the use of third parties in their privacy notice. Interface can provide a model privacy statement for practices to add into their privacy notices and will support practices if they get questions from patients about third party access. | This risk is therefore significantly reduced and accepted. | There is a clear legal basis for third party access to the patient data and confidentiality is assured. The final impact on individuals is justified so long as the practice privacy notice indicates that third parties may review patient data to support the direct care of patients.  |  |

  |

DPO sign off

MILLION, Caroline (NHS SOUTH YORKSHIRE ICB - 03N)













To:

* FELLS, Rose (THE SCOTT PRACTICE)

Wed 12/28/2022 11:47

Hi Rose

I can confirm that I am happy with this DPIA.

Regards

Caroline

Caroline Million
Independent DPO and IG Specialist

email: caroline.million@nhs.net
tel: 07912975522

1. https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-by-design/ [↑](#footnote-ref-1)
2. Registration number:Z2172212 [↑](#footnote-ref-2)
3. All patient identifiable data is removed other than a reference number that Interface cannot use to re-identify patients, for example, EMIS number or SystmOne reporting ID [↑](#footnote-ref-3)