Data Protection Impact Assessment contract to undertake health assessments for registrants

Data Protection Impact Assessment Screening Questions			
Contact name and job title		Shugafta Akram – Head of Fitness to Practise (FtP) Change, Quality and Continuous Improvement	
Description of New project, system, technology or legislation name being assessed		Contract to undertake health assessments for registrants involved in our FtP investigations.	
Purpose/Objectives of the initiative (if statutory, provide citation)		**The outsourcing and provision of registrant medical information to consider whether they would have a detrimental effect on their fitness to practise.** **Rule 3 – requires the registrar to consider any concerns that are raised or referred relating to the fitness to practise of the registrant.** **Section 33(b) the registrar may seek information to assist it in making it's decision/ investigation.** **Section 36(y) relates to DCP and is same as above section.**	
	DPIA Question	**Answer and details**	**Proposed mitigations/recommendations**
1	Will the project process special-category data or criminal-offence data on a large scale	Yes – health data/ genetic data of registrants	High risk. Need to ensure relevant security is put in place and contractors have suitable protections
2	Will the project involve a change to the nature, context purpose or scope of our existing personal data processing?	No – contractual alteration rather than a process change, although subcontractors will also be used by the service provider.	N/A
3	Will the project process personal data that could result in a risk of physical harm in the event of a DSI?	Yes – loss, erasure or breach of medical data in the event of a DSI would potentially cause distress and anxiety to registrant	High risk – especially with the transfer of data, Adequate security needs to be put in place through the communication and storing processes.

4	Will the project use innovative technology in combination with any of the criteria in the European guidelines	No – medical testing and processing of information only	N/A
5	Does the project carry out profiling on a large scale, use automated decision making for special category data or make significant decisions about people, including access to a service opportunity or benefit?	No	N/A
6	Does the project combine, compare or match data from multiple sources?	Yes – various data controllers will be inputting or providing information either through testing or records provided by the registrant's GP/psychiatrist etc.	High risk – checks need to be put in place to ensure that only the information necessary for the FtP process is colelcted, the accuracy of the information, the storage and transition. This may require a new process or checklist
7	Does the project process personal data without providing a privacy notice directly to the individual in combination with any of the criteria in the European guidelines	No	N/A
8	Will the project process biometric. health or genetic data in combination with any of the criteria in the European guidelines	Yes	See comments from Box 1
9	Does the project process personal data in a way that involves tracking individuals' online or offline location or behavior, in combination with any of	No	N/A

	the criteria in the European guidelines?		
10	Will the project process children's personal data for profiling or automated decision-making or for marketing purposes, or offer online services directly to them?	No	N/A
11	Will the project systematically monitor a publicly accessible place on a large scale?	No	N/A

Need for DPIA identified? If yes, then explain reasons (refer to screening questions above). If a DPIA is not to be carried out the reasons should be documented. Please note, consideration for a DPIA should still be given even if none of the above questions are answered 'Yes'.

Yes. The work involves the collection and use of special category data, in relatively high volumes and at a level that may pose a risk to the rights of the data subjects if not sufficiently managed and mitigated.

Completed by:

Colin Lench

Signed: Date:

Data Protection Impact Assessment

Contact name and job title	Shugafta Akram – Head of FtP Change, Quality and Continuous Improvement
Description of New project, system, technology or legislation name being assessed	Contract to undertake health assessments for registrants involved in our FtP investigations.
Purpose/Objectives of the initiative (if statutory, provide citation)	Rule 3 – requires the registrar to consider any concerns that are raised or referred relating to the fitness to practise of the registrant. Section 33(b) the registrar may seek information to assist it in making it's decision/ investigation. Section 36(y) relates to DCP and is same as above section.

1. Why do we need a DPIA?

What are the overall objectives of the project and what type of processing does it involve? Consider including a link to the business case

Identify through medical records/history information which could influence a registrant's fitness to practise. This will be used alongside other information which the GDC will carry out for its FtP investigations.

This involves the processing of sensitive personal data and an agreement to be put in place with Heales, an outside organization that specializes in this area of work. Heales, along with the GDC determine the purposes and means of processing. Although the external organization would be a controller in their own right and liable in the event of a breach attributable to its actions there would still be a risk to the registrants well-being in the event of breach, In addition, the GDC would have reputational damage, cost implications in event of breach if it was found to be negligence on the GDC's part.

This project is not a change to any existing process but simply a change to a new provider who may process data differently although the purpose of the processing remains the same. Further information attached to business case below:

Business Case

The processing of personal data for both the GDC and external provider involves special category data and involvement of third parties such as doctors, psychiatrists, specialist health advisors and external processors who undertake the necessary tests.

The classes of data include names, date of birth, addresses, (private and work addresses) telephone numbers, email and mobile telephone numbers. It will also include sensitive data such as medical records from GP/ Hospitals/blood tests, hair samples.

2. Describe the processing

What is the nature of the processing

How will the GDC collect, store and delete the data? Who will the GDC be sharing data with? Are there sufficient agreements in place? Does the project involve new or inherently privacy-invasive technologies? Does the project involve new or substantially changed identity authentication requirements that may be intrusive or onerous? Which of the processes are high risk? Consider including flow diagrams or links to any data mapping.

This process involves the assessment of medical records to support the GDC in its decision making for fitness to practise cases.

The GDC informs the registrant that it is exercising its legal duty under Section 33(b) of the Dentist Act 1984 (as amended) to assist it in its investigations and obtain medical records. These can either be existing medical records depending on the nature of the issue or involve arrangement of carrying out of the medical tests on the registrant. The GDC would provide the registrant with its privacy notice either through a link or hard copy depending on the method of communication. The contractor's privacy notice would also be provided at the outset. The lawful basis of process for the special category information would be the GDC's regulatory function and substantial public interest.

The registrant would then confirm to proceed with the health assessment, complete and send an online referral form or provide a medical reference(s). The online portal would be accessible to the GDC and the contractor. The contractor would conduct an initial screening, state what kind of assessment is needed and either obtain the medical records or arrange the relevant testing. However, in the event the registrant would refuse to agree to the tests or provide medical records then the GDC will record this as a 'refusal to co-operate'.

Following the initial screening, the contractor will state what further assessment is needed and inform the GDC via the online portal or secure email. The contractor will then carry out further screening, either obtaining the medical records from the registrant's GP or medical records or arrange with its sub-processor the arrangements to undertake additional tests. The processor would be working on behalf of the contractor.

The contractor would be responsible for the gathering and storage of the registrant's personal data for the processing on its part. Processors working on behalf of the contractor would use its systems and not hold any data separately apart from medical samples. Medical data such as hair and blood samples will be destroyed within a few days of the testing. Existing medical records will be obtained from the registrant's doctor/ psychiatrist etc. by the contractor depending on the nature of the investigation. Blood samples and other testing materials will be destroyed after a period of a week.

Registrants can challenge the results of the tests if they believe they are inaccurate or ask for an additional test, exercising their right to rectification.

The contractor will hold the data for a period of up to six years after the end of the contract.

The contractor will provide a report to the GDC for its deliberations. The information will be stored on the GDC's CRM system which ensures access is only to the relevant teams. The information will be accessed by all teams within the GDC involved with the case handling in line with its privacy statement. All emails containing special category or sensitive personal data between the GDC and Heales will be sent securely either through Secure file or encrypted.

Further information on the processing can be accessed via the link below.

Processing

The GDC will hold the information in line with its retention policy which can be accessed via the link below.

Retention Policy

What is the scope of the processing?

What is the type of data? Is it special category data **(**race; ethnic origin; political views; religion; trade union membership; genetics; health; sex life; sexual orientation or biometrics (if used for ID purposes)). Does the project involve an additional use of an existing identifier for single or multiple purposes? What are the volumes of data being collected? How many individuals will it affect? What is the retention of the information? Will the project result in the handling of a significant amount of new data about each person or significant change in existing data holdings?

This project will involve the collection, sharing and storage of personal data of registrants. The table below shows what data we will be processing. Please note, for each investigation we would only be collecting what is necessary to carry out the

Registrant data category*

Data category	**Justification**
Name	Identification
Address	Identification
Post code	Identification
Business address	Identification / contact
Gender	Assessment
Telephone number	Contact
Mobile number	Contact

Date of birth	Assessment/identification
Email address (home)	Contact/ identification
Email address (business)	Contact/ identification
Registration number	Identification
Medical history	Investigation
Complaint (if applicable)	Investigation
Blood tests	Investigation
Hair samples	Investigation
Other specialist medical information	Investigation
Opinion of registrants ability to practise	Review process

The investigation process would involve only the gathering of data from the registrant. This data will be kept to the minimum of only enough to carry out the investigation and no more. This follows the GDC's previous investigative process. The volume of the data will only cover the individual registrant within the UK. We expect this processing to be no more than a two hundred data subjects per year. This information is sensitive and contains medical history of the registrant. We estimate the length of time for the processing to be the history of the FtP investigation and the information to be stored in line with the GDC's retention policy. It will be stored by Heales in line with its own policy of six years after the end of the contract.

What is the context of the processing?

What is the relationship between the GDC and the data subjects? What control will the data subjects have and do they include vulnerable groups and children? Are there any security flaws and what are the technological capabilities in this area? Are there any concerns that the GDC should consider? Are any certifications required or codes of conduct?

As the Regulator for the dental profession in England and Wales the GDC processes substantial data of its registrants. It has a statutory duty to maintain standards in UK dentistry.

In some circumstances, it will investigate registrants' fitness to practise. This may include health information so registrants may be in a vulnerable position depending on their situation. This is a long-standing process the GDC has carried out over several years.

Registrants can refuse to have their data processed and the investigation can be carried forward without a health assessment. However,

this would lead to the GDC alleging lack of co-operation.

All information will be stored and transferred by all parties securely. The contractor and its processors are contractually and legislatively obliged to ensure the data it stores and transfers is secure.

What are the purposes of the processing?

What do we want to achieve from the processing? What benefits will it deliver and who will receive these benefits?

The GDC has a statutory duty to regulate dentistry in the UK and ensure patients are protected. One of the tools we do this is through our FtP investigation process. This process helps ensure that no registrants providing a service to the public pose a risk.

By ensuring registrants are fit to practise we help give the public confidence in UK dentistry. We also help to maintain the standards of registrants and ensure the industry is fit for purpose.

3. Consultation process

How will we consult with stakeholders?

When and how will we seek the views of individuals? Will it be through newsletters or more formal consultation and involve end users or processors? Will we require expert advice on any areas such as IT? If we decide not to consult what reasons do we have?

This is an existing process and as it is part of our statutory responsibility there is no necessity to consult registrants. This work involves processing the personal and special category information of a very small percentage of registrants. The GDC would need to continue to carry out this work as part of its role as the regulator of the dental profession even if stakeholders objected.

Consultation would be a lengthy exercise and disproportionate when comparing the number of registrants to the number of FtP cases. Consulting on this process would also risk undermining the GDC's role as the regulator and the FtP process.

The roles and responsibilities between the GDC and the contractor are identified within the contract.

4. Necessity and proportionality assessment

What are the measures of proportionality and compliance?

What are our lawful basis of process and does it achieve our goals? Is the justification for the new data handling unclear or unpublished? Are there better or more secure ways we can do this? Is it futureproof and what are we doing to avoid function creep? How will we approach data minimization and data quality? What information will we be sharing with individuals?

This process helps ensure all factors are taken into consideration when the GDC assesses a registrant in the FtP process. There are no alternatives to processing this way. Medical records may identify some underlying issues but in some cases FtP would require more up to

date information for the testing in some cases.

The lawful basis of the GDC processing this information are a legal obligation under the Dentists Act 1984 (as amended). We process special category data (health and genetic data) under the lawful bases of:

Reasons of substantial public interest 9(2)(g) – regulatory requirements

Information is explained further in the GDC Privacy Notice.

Registrant details are held by the GDC for its normal day to day duties. Medical information will only stored and processed for the FtP purposes. Only the information needed to carry out the investigation will be collected by the contractor For example, an investigation would some but not all medical records of a registrant.

The information collected by the contractor will be for identification of the registrant and to enable us to make contact(s). We will be collecting various sources of data depending on the registrant's preferred method of contact.

There will be no other purposes for the collection of this information. It will not be held longer than is stated in the retention policy of either the GDC or the contractor. The contractor will be responsible for its processors retention periods of the test data. All other information will be processed within Heales systems which its processors will input information into.

In the event of any procedural changes then this will be reviewed and any changes made will be included in a new DPIA if it is not suitable to update this document.

5. Data security

Assess the levels of security of the project

How will we ensure personal data will be stored and processed securely? Will this require additional security measures? Will we require external advice? How will we ensure processors are compliant. What steps will we need to take in the event data is transferred between systems or internationally?

All of the processing will be carried out within the EU so there will be no sovereignty issues.

The personal data will be checked by the contractor who will have their own process to ensure accuracy. Due diligence is included in the contractual terms under section 2.1.1. where it will undertake the any checks on data provided to it by the GDC is accurate. Under Section 15 and 16.7 and 16.8 the contractor has also committed to protect the personal data it holds.

Under section 16.7.5 of the contract, Heales has also committed to store data on a secure system that complies with the security system that reasonably complies with the requirements of the GDC.

In the event of loss or breach Heales are covered by an indemnity of up to £5million.

The GDC will store the information on its systems in line with its information security policies.

GDC information security policies

6. Risk assessment

Describe the source of the risk and potential impact on individuals. Include mitigation measures where the risk identified is medium or higher. In the event a high risk cannot be mitigated adequately, it may be necessary to consult with the ICO.

Risk and impact on individuals		Likelihood	Severity	Overall risk	Mitigation options	Effect on risk	Residual risk	Approved?
1.	Human error - where information is sent to unintended recipient	High	High	High	Training of staff/ 2 minute delay on emails/secure file share/ disable autofill	Reduce likelihood to low but severity would remain high	Medium / low	Yes/No
2.	Secure file share/portal compromised	Low	High	Low	IT security – firewalls Staff training Secure network / password protected / limited authorized users.	Reduce likelihood to low	Low	Yes/No
3.	Failure by the joint controller - lose personal data	Low	High	Low	Indemnity Controller liability	Reduce likelihood to low Although GDC	Low	Yes/No

						would have reputational damage		
4.	**Incorrect information received**	**Medium**	**High**	**Medium**	**Staff trained to identify errors** **Procedure to check information** **Breach would be on the contractor or third party**	**Reduce likelihood to low**	**Low**	**Yes/No**
5.	**Unnecessary sensitive information that we do not need for example religious belief or health information that we don't need etc**	**Low**	**Medium**	**Low**	**Staff trained to identify errors and also can filter out the unnecessary information and go back to sender** **Breach would be on the contractor or third party**	**Reduce likelihood to low**	**Low**	**Yes/No**
	Information lost by GDC	**Medium/ High**	**High**	**Medium/ High**	**Redaction / staff training on retention processes**	**Reduce likelihood to low**	**Low/ Medium**	

7. Sign off

Item	**Name/position/date**	**Notes**
Measures approved by:		Integrate actions back into project plan, with date and responsibility for completion

Residual risks approved by:		If we are accepting any residual high risk then we should consult the ICO before continuing
DPO advice provided	Luke Whiting 04.12.19	DPO should advise on compliance, mitigations and whether processing should proceed
There are clear and significant data privacy and security risks associated with the collection and processing of special category data of type and scale envisaged. However, these can be appropriately mitigated by the controls and processes the GDC and Supplier have identified as having in place or plan to put in place before work starts (outlined in compliance check below and the process map linked to above). However, the contract and arrangements do need to be tightly managed on an ongoing basis once the contract is agreed to ensure not only the procured service is being provided, but that is being provided safely and securely and in the way we have agreed. Data security concerns should be fed back to the supplier as they arise and should bey a key aspect of the way in which the delivery of the contract and the suppliers performance is monitored and assessed.		
DPO advice accepted or overruled by:		If overruled, please explain your reasons
Comments:		
Consultation responses		In the event the decision differs from respondents

reviewed by:		we should explain our reasons
Comments:		
This DPIA will be kept under review by:		The DPO should also review ongoing compliance with the DPIA

Data Protection Act Compliance Check			
		Details	Action required
1	***Principle (a) – Lawfulness, fairness and transparency*** ***Personal data shall be processed fairly, lawfully and, in a transparent manner in relation to the data subject processed unless: a) at least one of the conditions in Schedule 2 is met, and b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.***		
		Details	Action required
1.1	Have you identified specific grounds for processing (these should follow the six bases for processing data). If no lawful basis applies, then this principle will be breached.	Yes Article 6 legal requirement ?	Confirmation that all parties are content with the lawful basis of processing.
1.2	Does this project involve handling of special category data? If yes, then this will require one of the 10 lawful bases of processing special category data. Please list the categories and the lawful basis of process	Yes Article 9 significant public interest for the FtP investigations – regulatory duties.	Agreement that all parties are content with the lawful basis of processing of special category information.
1.3	Does the processing result in other unlawful activities (such as copyright Human Rights Act 1998 etc.?	No	N/A
1.4	Will we be processing personal data in a way in which the subjects would expect?	Yes	Registrants will be advised how their data will be processed and their personal data will not be processed in any way other than for the purposes of the investigation

1.5	How will we inform the data subjects of the processing of their data? (This could be through our privacy statement or if applicable when we obtain consent	Through the privacy statement of the GDC when advising the registrant of the planned processing. This will also be provided by Heales.	Ensure that providing privacy notices in included in the process.
1.6	If you are relying on consent to process personal data, how will this be collected and what will you do if it is withheld or withdrawn?	We are not using consent or explicit consent for this process.	N/A
1.7	Do you need to amend your privacy notices? If yes, please describe how.	No	No
2	***Principle (b) - Purpose limitation***		
		Details	Action required
2.1	Does the project involve the use of existing personal data for new purposes?	No, this follows an existing process and we are only changing the contractor to carry out the medical examinations for FtP complaints	N/A
2.2	How is the use of existing personal data for new purposes being communicated to (a) the data subject; (b) the person	N/A	N/A
2.3	Are the new purposes compatible with the original intentions?	N/A	N/A
2.4	Are these new purposes fair, lawful and transparent in accordance with Principle (a)?	N/A	N/A
3	***Principle (c) - Data minimisation***		
		Details	Action required

3.1	Is the personal data sufficient to serve its intended purpose? good enough for the purposes it is used?	Yes – only enough data will be processed to obtain the medical investigation for the FtP case. Information will not be collected if it is unnecessary. Registrants will be contacted for identification and via their preferred contact method	Ensure throughout the process we are only using the minimal amount of information for processing.
3.2	Which personal data could you not use, without compromising the needs of the project?	Some contact details which would not be necessary if not going to be used.	None
4	***Principle (d) - Accuracy***		
		Details	Action required
4.1	How are you ensuring that personal data obtained from individuals or other organizations is accurate?	Data will be used from GDC sources and checked with Heales' processes. Heales will carry out the necessary checks	Check the processes and wording of the contract.
4.2	What steps will we be taking to delete or correct inaccurate personal data?	Both the GDC and Heales will be data controllers and will advise registrants of their rights to rectification through the respective privacy notices. In the event a registrant believes their information is inaccurate then they can request an additional test	Ensure there is an agreed process in the event a registrant challenges the accuracy of the data held.
4.3	Will we need to carry out regular checks or updates to ensure data is accurate?	No. The testing process through the contract is only a short term procedure. Registrants may challenge results but there is no necessity to undertake regular checks on data accuracy in addition to the QA and assurance surrounding the testing process	N/A
4.4	Will we need to include a procedure in the event of a challenge to the accuracy of the data?	Yes	Should be included in the terms of the contract
5	***Principle (e)*** - ***Storage limitation***		

		Details	Action required
5.1	What retention periods are suitable for the personal data you will be processing? If being used and shared with third party partners, how long will they retain the information for?	Retention period is set out in GDC and Heales policies. Links included in the DPIA	None
5.2	Will we need to review the retention periods and will this project cause any issues with our existing retention periods?	No	None
6	***Principle (f) - Integrity and confidentiality***		
		Details	Action required
6.1	Do we have appropriate security measures in place to protect the personal data we hold?	Yes Information security policy link included in the DPIA. Other information is stored securely in line with existing policies. Heales has its own security policies and would be liable in the event of a breach on its side.	Nothing outside the usual regular review of existing policies.
6.2	Are any risks suitably accounted for? Do we need to consider mitigation measures?	Risks included in the DPIA which will be regularly monitored and mitigated.	Continue to assess potential risks
7	***Accountability***		
		Details	Action required
7.1	Will we have sufficient policies and procedures in place when the project is implemented?	Yes this is a continuation of previous work but just undertaken by a different supplier.	None
7.2	Will staff need additional training?	Yes	Training/advice for the portal provided by the supplier.

7.3	Will we need to undertake regular checks to ensure the outcome of the project remains fit for purpose?	No- although we will expect the joint controller to adhere to the terms of the contract.	

Conclusions

This can be procured and implemented without impact on the DPA rights if the agreed mitigations are implemented as expected and agreed.