Data Protection Impact Assessment (DPIA)

When to carry out a DPIA

The DPIA identifies and assesses privacy implications where information (data) about individuals is collected, stored, transferred, shared, and managed. It should be process rather than output orientated.

The purpose is to have the potential to detect and mitigate information risks, as well as to modify plans accordingly.

A PIA should be completed when the following activities occur:

- Developing or procuring any new programme, policy, procedure, service, technology or system ("project") that handles or collects information relating to individuals.
- Developing revisions to an existing programme, policy, procedure, service, technology or system which significantly change how information is managed.

The General Data Protection Regulation (GDPR) became law on 24th May 2016, is a single EU-wide regulation on the protection of confidential and sensitive information. It enters into force on the 25th May 2018, repealing the Data Protection Act (1998).

The Regulation in Article 35 (recitals **84, 89, 90, 91, 92, 93, 95**) makes it obligatory to perform a Data Protection impact assessment in case of large scale processing of special categories of data **(as in this case health data and genetic data see article 9(1)**. This could help to ascertain the legal basis for processing, which will be helpful for public authorities now that the open door of 'legitimate interests' is closed. It is also important to note that "a single assessment may address a set of similar processing operations that present similar high risks". This could significantly help in reducing the administrative burden for hospitals and health and care providers when performing such an \\assessment.

A data protection impact assessment shall in particular be required in the case of:

(a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;

(b) processing on a large scale of special categories of data referred to in **Article 9(1),** or of personal data relating to criminal convictions and offences referred to in Article 10; or

(c) a systematic monitoring of a publicly accessible area on a large scale.

This DPIA has been designed to meet the requirements of current legislation and common law duties and the expanded requirements of the GDPR as above, however Consent modelling / Fair Processing modification should be addressed by separate Trust GDPR action plans and strategies as several of the policies currently in use will need to be updated to reflect legislative changes.

Step 1 – EMIS WEB

Project name/title	**Transfer of EMIS web to AWS Infrastructure**
Description and purpose of the initiative – Include how many individuals will be affected by the initiative. A data processor acting on our behalf, EMIS Health, is changing certain technical aspects of the way in which it delivers services to us (see https://www.emisnug.org.uk/blog/next-generation-emis-x-announced), and as part of this transition it will be moving the data which it hosts on our behalf from its own data centre to a third party data centre, which is owned and operated by Amazon Web Services (AWS). Delivery of the services is subject to the terms of the GP Systems of Choice Framework (GPSOC) which is managed by NHS Digital on behalf of the Secretary of State for Health. The exercise will involve a change to the manner in which data is being processed on our behalf. Although this change does not introduce processing that is likely to result in a high risk to individuals (which would necessitate the undertaking of a DPIA), given that the data includes special category data we nevertheless feel that it is appropriate that we undertake a review.	
Details of any link to any wider initiative (if applicable)	N/A
Stakeholder Analysis List those who may be affected (stake holder have been consulted prior to project start), eg. Service Users, Clients, Staff-managers and practitioners, Trade Unions, Visitors, Professional organisations, IT providers, Regulators and inspectorial bodies, MPs, Councillors, Partner organisations, Media, Carers	**Internal: Partners** **External: EMIS/Patients**
Does the initiative involve the use of existing personal and/or confidential data: • **For new purposes?** • **In different ways?** **If so, please explain** (if not already covered above)	As detailed above, the data (which includes special category data (i.e. health data) which is collected via the processor's clinical IT system and which forms the patient's medical record) will be stored in a third party data centre (which will act on the instructions of EMIS Health, who in turn will act in accordance with instructions received from (or on behalf of) ourselves as the relevant controller pursuant to our call off contract under the GPSOC framework or as otherwise documented). Aside from the manner in which the data is being hosted, we have not identified, as part of this change, any material change to the manner in

	which the data is being processed (in terms of data sharing and/or use)
Are potential new purposes likely to be identified as the scope of the initiative expands?	No
What is already available? Any Previous PIA, Research or Consultation undertaken.	

Step 2 – Contacts

Who is completing this assessment?	
Name	Paul Couldrey
Job Title	Data Protection Officer
Department/Directorate name	
Contact address	Couldrey@me.com
Email address	Couldrey@me.com
Telephone number	07525 623939
Connection to Project	DPO for Practice

Step 3 – Screening Questions

The purpose of these questions is to establish whether a full Privacy Impact Assessment is necessary and to help to draw out privacy considerations					
		Yes	**No**	**Unsure**	**Comments - document initial comments on privacy impacts or clarification for why this is not an issue or why you are unsure**
I	Is the information about individuals likely to raise privacy concerns or expectations e.g. health records, criminal records or other information people would consider particularly private?		X		
ii	Will the initiative involve the collection of new information about individuals?		X		
iii	Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?		X		
iv	Will the initiative require you to contact individuals in ways which they may find intrusive[1]?		X		
v	Will information about individuals be disclosed to		X		

[1] Intrusion can come in the form of collection of excessive personal information, disclosure of personal information without consent and misuse of such information. It can include the collection of information through the surveillance or monitoring of how people act in public or private spaces and through the monitoring of communications whether by post, phone or online and extends to monitoring the records of senders and recipients as well as the content of messages

	organisations or people who have not previously had routine access to the information?				
vi	Does the initiative involve you using new technology which might be perceived as being privacy intrusive e.g. biometrics or facial recognition?	X			The scope of the data processing is as detailed in the relevant GP Systems of Choice contract (and related call off contract (and deed of undertaking)) or as otherwise agreed in writing between EMIS Health and ourselves. As noted above, aside from the hosting element the manner in which the data is being used or otherwise processed will not materially change as a result of this change
vii	Will the initiative result in you making decisions or taking action against individuals in ways which can have a significant impact on them?		X		
viii	Will the initiative compel individuals to provide information about themselves?		X		

If you answered **No** to all of the above screening questions, and you can evidence/justify your answers in the comments box above, you do not need to continue with the PIA.

Should the project at any point in the future use personal information you will need to revisit the screening questions and the PIA.

If you answered or **Unsure** to any of the above, please continue with the PIA.

Step 4 – Data Collection

Please mark all information to be collected

Description	Specific data item (s)	Justification Reason that the data item(s) is/are needed
Personal Details		
Family, lifestyle and social circumstances	Marital/partnership status Next of kin Carers/relatives Children/dependents Social status e.g. Housing	The lawful basis for processing (a mixture of consent, explicit consent, fulfilling public duties and providing direct healthcare) the patient records does not change as a result of this proposed change, the only difference is a technical one in terms of how the services is being delivered by the relevant processor (i.e. EMIS Health). We have in place a privacy notice which refers to the use of third party processors/service providers, which would include EMIS Health. We are informed that the data will not be transferred overseas in connection with this change of service. Strictly private & confidential 3 The processing which is undertaken by EMIS Health on our behalf is governed by the terms of the GP Systems of Choice Framework Agreement (together with the relevant Call Off Contract) which includes broad data protection obligations and we are able to directly enforce those obligations against the processor pursuant to a deed of undertaking which has been signed by EMIS Health and which each individual practice can rely upon

Description	Specific data item (s)	Justification Reason that the data item(s) is/are needed
Education and training details	Education/ Qualifications Professional training Not applicable	The lawful basis for processing (a mixture of consent, explicit consent, fulfilling public duties and providing direct healthcare) the patient records does not change as a result of this proposed change, the only difference is a technical one in terms of how the services is being delivered by the relevant processor (i.e. EMIS Health). We have in place a privacy notice which refers to the use of third party processors/service providers, which would include EMIS Health. We are informed that the data will not be transferred overseas in connection with this change of service. Strictly private & confidential 3 The processing which is undertaken by EMIS Health on our behalf is governed by the terms of the GP Systems of Choice Framework Agreement (together with the relevant Call Off Contract) which includes broad data protection obligations and we are able to directly enforce those obligations against the processor pursuant to a deed of undertaking which has been signed by EMIS Health and which each individual practice can rely upon
Employment details	Employment status **X** Career details **X** Other □ specify: Not applicable	As above
Financial details	Income □ Salary □ Bank details □ National Insurance number □ Benefits **X** Other □ specify: Not applicable	As Above
Sensitive Data: **Racial or ethnic origin**	X	As above

Description	Specific data item (s)	Justification Reason that the data item(s) is/are needed
Sensitive Data: Physical or mental health or condition NB. Includes treatment if applicable. Include Mental Health status eg. whether detained or voluntary under the Mental Health Act if applicable.	X	As above
Sensitive Data: Sexual identity and life	X	As above
Sensitive Data: Religious or other beliefs of a similar nature	x	As above
Sensitive Data: Trade union membership	Not applicable	As above
Sensitive Data: Offences including alleged offences	X	As above
Sensitive Data: Criminal proceedings, outcomes and sentences	X	As above

Describe 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?

As detailed above, the data (which includes special category data (i.e. health data) which is collected via the processor's clinical IT system and which forms the patient's medical record) will be stored in a third party data centre (which will act on the instructions of EMIS Health, who in turn will act in accordance with instructions received from (or on behalf of) ourselves as the relevant controller pursuant to our call off contract under the GPSOC framework or as otherwise documented). Aside from the manner in which the data is being hosted, we have

not identified, as part of this change, any material change to the manner in which the data is being processed (in terms of data sharing and/or use).

Describe the scope of the 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?

The scope of the data processing is as detailed in the relevant GP Systems of Choice contract (and related call off contract (and deed of undertaking)) or as otherwise agreed in writing between EMIS Health and ourselves. As noted above, aside from the hosting element the manner in which the data is being used or otherwise processed will not materially change as a result of this change.

Describe the context of the processing: 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? Are you signed up to any approved code of conduct or certification scheme (once any have been approved)?

This DPIA distinguishes between: (i) the day to day processing undertaken (by us as a controller and EMIS Health as a processor acting on our behalf (and which will not change and so is not covered in detail)); and (ii) the change to the manner in which the data is being hosted by or on behalf of the processor (and which is the focus of this DPIA). We are aware that cloud computing is an established technology and the adoption of which is something which is being driven within the public sector – https://www.gov.uk/guidance/use-cloud-first The use of cloud computing has been recognised by the Government as being beneficial because:

- you can avoid upfront investments in your infrastructure, reducing overall costs;
- there's greater flexibility to trial new services or make changes, with minimal cost;
- pricing models are scalable - instead of building for the maximum usage you buy for less usage and increase or decrease as appropriate;
- it will be easier to meet the Greening Government Commitments - cloud facilities typically try to use server space and power in the most efficient way possible;
- upgrades and security patches can be applied continuously; and
- the supplier will have responsibility for making sure the service has good availability for users.

In terms of issues of public concern, we understand that individuals may have an issue with their medical record being held by a commercial organisation but, the fact is that the relevant patient records are already being held by third party commercial organisations (either EMIS

or one of the other primary system suppliers under GPSoC (or by sub-processors acting on their behalf)) and the only real change here is the identity of the third party (i.e. the data is moving from a processor to a sub-processor). With regard to questions of security we are aware that the National Cyber Security Centre has issued guidance on cloud security - https://www.ncsc.gov.uk/collection/cloud-security and we understand that the relevant service provider in this instance (AWS) operates at the very highest levels of security (details of which are set out at https://aws.amazon.com/security/).

Describe the purposes of the processing: 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?

As noted under the question above, the move to a third party cloud environment is seen as beneficial for a number of reasons for us as a controller (in terms of improved availability, resilience and service in respect of the services being delivered to us by the processor) and in respect of the patients (in terms security, integrity and availability of their data).

Consultation process
Consider how to consult with relevant stakeholders: describe when and how you will seek individuals' views – or justify why it's not appropriate to do so. Who else do you need to involve within your organisation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts?

The GPSoC services are provided pursuant to a framework agreement as between NHS Digital and EMIS Health (with services then being purchased at a CCG level on our behalf as a service recipient). Under the terms of the GPSoC framework, NHS Digital essentially acts for and on our behalf in terms of approving the appointment of processors to the framework and, once they are appointed, the use of any subcontractors (and so sub-processors). We understand that EMIS Health has engaged with NHS Digital in order to secure a variation to the framework agreement to provide for the appointment of AWS as an approved material sub-contractor. EMIS Health has notified the relevant GP practices, including ourselves, so that we have an opportunity to raise any concerns with regard to the proposed change but as this change is a universal technical/operational change it is more appropriate for such matters to take place at a framework level (which is why the GPSOC Framework Agreement is structured as it is). In any event, the Guidance issued by the ICO would suggest that this is a move which the processor is entitled to drive on its own behalf provided that it remains within the scope of the relevant contract (i.e. in its Controller/Processor detailed guidance the ICO states "In certain circumstances, and where allowed for in the contract, a processor may have the freedom to use its technical knowledge to decide how to carry out certain activities on the controller's behalf.").

Assess necessity and proportionality
Describe compliance and proportionality measures, in particular: what is your lawful basis for processing? Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep? How will you ensure data quality and data minimisation? What information will you give individuals? How will you help to support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfer?

The lawful basis for processing (a mixture of consent, explicit consent, fulfilling public duties and providing direct healthcare) the patient records does not change as a result of this proposed change, the only difference is a technical one in terms of how the services is being delivered by the relevant processor (i.e. EMIS Health). We have in place a privacy notice which refers to the use of third party processors/service providers, which would include EMIS Health. We are informed that the data will not be transferred overseas in connection with this change of service. The processing which is undertaken by EMIS Health on our behalf is governed by the terms of the GP Systems of Choice Framework Agreement (together with the relevant Call Off Contract) which includes broad data protection obligations and we are able to directly enforce those obligations against the processor pursuant to a deed of undertaking which has been signed by EMIS Health and which each individual practice can rely upon.

Identify and assess risks

Describe the source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary	Likelihood of harm (Remote, possible or probable)	Severity of harm (Minimal, significant or severe)	Overall risk (Low, medium or high)
Loss of data in the transfer of data to the sub-processor	[Remote]	[Severe]	[Medium]
Misuse of data by the sub-processor	[Remote]	[Severe]	[Medium]

Identify measures to reduce risk Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step above

Risk	Options to reduce or eliminate risk	Effect on risk	Residual Risk	Measure approved
Loss of data in the transfer of data to the sub-processor	We are informed that the data will be transferred in a very secure manner and in any event EMIS Health will retain a copy of the data in its current hosting centre unless or until there is evidence that all of the relevant data has been transferred.	[Reduced]	[Low]	**DPO 03 June 2019**
Misuse of data by the sub-processor	We are informed that the way in which the AWS service operates means that there is no opportunity for AWS employees to access or view the data held within the EMIS Health allocated areas of the hosting service. The data will be encrypted both at rest and in transit and AWS will not have access to the encryption keys. See https://aws.amazon.com/security/ for further details). AWS already provides numerous services to Governmental organisations (such as Crown Commercial Services and the Ministry of Justice (see - https://aws.amazon.com/solutions/casestudies/uk-moj/) who will have undertaken their own detailed assessments.	[Reduced]	[Low]	**DPO 03 June 2019**

References

- Data Protection Act 1998;
- General Data Protection Regulations 2016
- The Caldicott Principles;
- Common Law Duty of Confidentiality;
- The Freedom of Information Act 2000;
- The Mental Capacity Act 2005;
- Section 251 of the NHS Act 2006 (originally enacted under Section 60 of the Health and Social Care Act 2001);
- Public Health (Control of Disease) Act 1984;
- Public Health (Infectious Diseases) Regulations 1988;
- The Gender Recognition Act 2004;
- Confidentiality: NHS Code of Practice 2003;
- IGA Records Management Code of Practice for Health and Social Care 2016;
- Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 2013;
- Abortion Regulations 1991;
- Road Traffic Act 1988;
- ICO Data Sharing Code of Practice;
- Confidentiality and Disclosure of Information Directions 2013;
- Health and Social Care Act 2012;
- The Criminal Justice Act 2003;
- The NHS Information Security Management Code of Practice 2007;
- The Computer Misuse Act 1990;
- The Electronic Communications Act 2000;
- The Regulation of Investigatory Powers Act 2000;
- The Prevention of Terrorism Act 2005;
- The Copyright, Designs and Patents Act 1988;
- The Re-Use of Public Sector Information Regulations 2005;
- The Human Rights Act 1998;
- The NHS Care Record Guarantee 2007; and
- Anonymisation Standard for Publishing Health and Social Care Data Code of Confidentiality.