Strictly private & confidential

OAKWOOD MEDICAL CENTRE

Draft example DPIA (provided as a suggested example to aid customers' drafting their own assessments)

Data Protection Impact Assessment

Step 1: Identify the need for a DPIA

Explain broadly what the project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA.
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.

Step 2: Describe the processing

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 scaleable - 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).

Step 3: 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 sub-contractors (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.*").

Step 4: 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 transfers

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 **<add in link or attach copy>** 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.

Step 5: 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]

Step 6:

Identify measures to reduce risk Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5

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]	[Y]
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/case-studies/uk-moj/) who will have undertaken their own detailed assessments.	[Reduced]	[Low]	[Y]

Step 7:

Item	Name/Date	Notes
Measures approved by:	DR. N. LUTY 7/6/19	Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:	DR. N. LUTY 7/6/19	If accepting any residual high risk, consult the ICO before going ahead

DPO advice provided:		DPO should advise on compliance, step 6 measures and whether processing can proceed
Summary of DPO advice [From the information provided by EMIS Health, we are satisfied that the security; availability; integrity and confidentiality, of the patient data will improve as a result of the move to the AWS data service. As noted above, the ICO guidance states that a processor has the ability to decide certain technical aspects of the processing, including "how the data is stored". This change does not affect the underlying processing and the manner in which the processing is controlled by the practice (either directly or indirectly via NHS Digital) and from the practice's and patient's perspective nothing will change as a result of this technical/background switch.]		
DPO advice accepted or overruled by:		If overruled, you must explain your reasons
Comments:		
Consultation responses reviewed by:		If your decision departs from individuals' views, you must explain your reasons
Comments:		
This DPIA will be kept under review by:		The DPO should also review ongoing compliance with DPIA

For the avoidance of any doubt, the information given in this document is for guidance and information only and does not constitute legal or professional advice. Always consult a suitably qualified information governance specialist and/or your own data protection officer in relation to the drafting of any Data Protection Impact Assessment (and/or in order to meet any of your other accountability obligations) in order to come to your own conclusions. EMIS Health assumes no responsibility for the information contained in this document and disclaims all liability in respect of such information.