Data Protection Impact Assessment (DPIA)

Building in Privacy By Design

This template is based on an ICO example of how to record your DPIA process and outcome. It follows the process set out in our DPIA guidance, and should be read alongside that guidance and the Criteria for an acceptable DPIA set out in European guidelines on DPIAs.

You should start to fill out the template at the start of any major project involving the use of personal data, or if you are making a significant change to an existing process. The final outcomes should be integrated back into your project plan.

Step 1: Identify the need for a DPIA
Explain broadly what 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.
The Health Information Exchange (HIE) is part of the Great North Care Record (GNCR) strategy: https://www.greatnorthcarerecord.org.uk/ Particular focus on HIE at: https://www.greatnorthcarerecord.org.uk/information-for-care-professionals/health-information-exchange/ A DPIA is required due to processing large volumes of special category data, and data matching between LAS (Sunderland's LiquidLogic case management system for Adult Social Care), and NHS Systems to populate the HIE interface.

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 other way of describing data flows. What types of processing identified as likely high risk are involved?
Social Care client data will be processed on LAS as per Sunderland's current arrangements and processes. Sources for the data will be the clients themselves, other professionals involved with them (GPs, Hospitals etc) LAS client data will be matched with NHSA native IT systems through NHS Number and Date of Birth (detailed example around Master Patient Index at **https://www.greatnorthcarerecord.org.uk/hie-update-may/)** Data transfer via on HSCN connection (Sunderland connection due June 2020)

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?
Key element is data necessary for the delivery of Adult Social Care, which obviously includes special category data, as outlined in ASC privacy notice (see Step 4). HIE covers the 3.6million people living in the North East and North Cumbria. Information team can provide Sunderland-specific indicative volumes for ASC ASC Retentions apply: https://www.sunderland.gov.uk/media/19514/Adult-Social-Care/pdf/Adult_Social_Care.pdf?m=636428174689230000 HIE Retention: "Deletion of information is the responsibility of the data source which will cascade through the HIE – where necessary a manual intervention will ensure that any centrally held data is also removed" *[Source: 191027 HIE DPIA v1.1*]

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)?
The controller needs to process personal information about the data subjects to deliver adult social care to them as clients, while fulfilling its ASC duties within the framework of relevant legislation, including: Health & Social Care Act 2012, Care Act 2014, Mental Health Act 2006, Safeguarding Vulnerable Groups Act 2006 As ASC clients, the data subjects are informed that the controller is unable to deliver ASC without the necessary information, and that they retain rights as outlined under Articles 12-23, via a privacy notice (see step 4) Aligned to this, there is a concern that references in HIE materials to opting-out of (e.g. https://www.greatnorthcarerecord.org.uk/opt-out/) provide an 'illusion' of consent – i.e. data subjects could misinterpret that consent is the lawful basis and they can withdraw consent. Sunderland PN (example at step 4) will instead refer to rights to object and restrict in effort to avoid any ambiguity around the degree of control the data subjects have.

GNCR is in second wave of LHCRE sites with Share2Care and the South West region, following first wave: Greater Manchester, Wessex, One London, Thames Valley, Yorkshire and Humber

SCC is registered as a data controller with the ICO (expires Nov 2020), and accredited on the NHS DSP Toolkit (renewal due Sept 2020). ICT currently accredited ISO 27001, NCSC Cyber Essentials.

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?

[Source: 191027 HIE DPIA v1.1]

"Providing health and social care professionals across North East and North Cumbria access to securely share patient's medical information electronically. The HIE solution will facilitate the electronic sharing of patient health records and information across the North East and North Cumbria Region. The Great North Care Record is a new way of sharing medical information across the North East and North Cumbria, which will be accessed by authorised health and social care practitioners.

It means that key information about patient health such as diagnoses, medications, details of hospital admissions and treatments is shared between different healthcare services including hospitals, out of hours and ambulance services who could be involved in the patient care.

The HIE brings together patient data across the health and social care systems in a secure manner, embedding a single aggregated longitudinal view of the patient natively in each EHR system. This is joined-up, safe and effective healthcare across organisational and system boundaries.

Currently, local health and ASC services hold various pieces of information about a patient's health which is spread over a number of systems. The HIE will provide a link to some of this key data by implementing a single point of access for health and social care professionals to use.

Benefits:

- Improve health care quality and safety
- Reduction in medication and medical errors
- Reducing duplicate and unnecessary paperwork
- Provides a more effective decision support for clinical staff
- Reduces redundant or duplicate testing
- Reduces inpatient hospital days and shorter length of stay
- Improves patient experience by reducing their frustrations during interviews and repeated questions
- Clinical staff devoting more time to care
- Records handled in a safe, secure and confidential manner
- Reduction in number of referrals
- Improve the public health information infrastructure "

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?
This is a collaborative piece of work for the region; full list of participating organisations at: https://www.greatnorthcarerecord.org.uk/information-for-care-professionals/health-information-exchange/ The Newcastle Upon Tyne Hospitals (NUTH) are leading the procurement, will own the contract and manage it on behalf North East and North Cumbria participating Health and Social care organisations. Key processors are Liquid Logic (LAS) and Cerner (HIE) https://www.liquidlogic.co.uk/adults/shared-care-records/ https://www.cerner.com/gb/en/solutions/health-information-exchange Individual views: https://www.greatnorthcarerecord.org.uk/?article=findings-yougov-poll https://www.greatnorthcarerecord.org.uk/wp-content/uploads/2018/09/GNCR-public-engagement-report-FINAL.pdf

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?
Lawful basis is derived from Article 6(1)(e) – processing necessary for the performance of tasks carried out in the public interest, or exercising official authority vested in the Council. Lawful basis for processing special category information derived from Art 9(2)(h) - the provision of health or social care or treatment, or the management of health or social care systems and services. Existing methods for sharing information between organisations involve electronic and physical transportation of records; HIE will allow for information to be accessed in more secure and timely manner. Ongoing engagement with public and participating organisations to review purpose and goals: https://www.greatnorthcarerecord.org.uk/information-for-care-professionals/data-ethics-and-ig/ LAS - Access controls in place, regular audit of user transactions on system by ASC information team. Data Quality programme for LAS, includes data clinics, Business Objects and in-house DQ reporting Liquid Logic have identified data fields for HIE Cerner interface; SCC can minimize these fields once they have been assessed but cannot augment. Information to data subjects via updated ASC Privacy Notice to include text around HIE/GNCR; Privacy Notice signposts to GNCR website. Draft processor contract with Cerner includes clauses to address requirements of Articles 28(3) and 32. Associated supplier questionnaire requires Cerner to document an overview of the technical and organisational measures they have in place. Business Continuity plan for ASC in place; LAS backup schedule in place.

Step 5: Identify and assess risks			
Describe 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
Fair, lawful and transparent			
Issue with legal basis. E.g. if consent-based processing, consent was not obtained and recorded. ***In this case, perception of such, based on use of term opt-out (see section 2 context)***	**Possible**	**Severe**	**High**
Privacy Notice not given.	**Possible**	**Severe**	**High**
Purpose			
Function Creep	**Possible**	**Severe**	**High**
Unauthorised access by third party/employee.	**Possible**	**Severe**	**High**
Data minimisation			
Too much data collected that's not necessary.	**Possible**	**Significant**	**High**
Data accuracy			
Inaccurate data collected locally and fed into HIE	**Possible**	**Significant**	**High**
Retention and disposal			
Data kept for too long.	**Possible**	**Significant**	**High**
Security			
Access controls not in place.	**Remote**	**Significant**	**Medium**
Monitoring and audit controls not in place.	**Remote**	**Significant**	**Medium**

Encryption, malware controls, patching, virus protection etc. not in place.	**Remote**	**Significant**	**Medium**
No written information sharing agreement in place with joint controllers.	**Remote**	**Significant**	**Medium**
No written contract in place with data processors.	**Remote**	**Significant**	**Medium**
No BCP, recovery plan or backups in place.	**Remote**	**Significant**	**Medium**
Staff not adequately trained/unfamiliar with new system	**Possible**	**Significant**	**Medium**
Data subject rights			
Data subject requests are not responded to in required timescales	**Remote**	**Severe**	**High**
Data can be restricted (if applicable).	**Remote**	**Severe**	**High**
Transfer outside EU			
Data transferred or stored outside EU e.g. in cloud without adequate safeguards.	**Possible**	**Significant**	**High**
Backups held outside EU, without adequate safeguards.	**Possible**	**Significant**	**High**

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** Eliminated Reduced Accepted	**Residual risk**	**Measure approved**
Illusion of consent, based on use of term opt-out	SCC privacy materials to avoid use of term opt-out	**Reduced**	**Low**	**Y**
Old PN issued	Comms to ASC and IG leads to approve and disseminate new PN with HIE text	**Reduced**	**Low**	**Y**
Function Creep	Purpose stated in PN. Ongoing engagement with GNCR Project Board to ensure adherence to purpose limitation	**Reduced**	**Low**	**Y**
Unauthorised access by third party/employee.	Review LAS technical and organisational access controls, audit programme.	**Reduced**	**Low**	**Y**
Too much data collected	Review LL field list against provisional areas outlined by operational lead	**Reduced**	**Low**	**Y**
Inaccurate data collected	Review Data Quality programme in context of data matching requirements. Review process for data correction where notified by joint controller.	**Reduced**	**Low**	**Y**

Data kept for too long.	ASC retentions in scope of ROPA review 2020; confirm HIE retention	**Reduced**	**Low**	**Y**
Access controls not in place.	Review LAS technical and organisational access controls, audit programme.	**Reduced**	**Low**	**Y**
Monitoring and audit controls not in place.	Review LAS technical and organisational access controls, audit programme.	**Reduced**	**Low**	**Y**
Encryption, malware controls, patching, virus protection etc. not in place.	ICT to review HSCN connection requirements and agreement, including context of mobile/home working arrangements for Covid19 measures.	**Reduced**	**Low**	**Y**
No written information sharing agreement in place with joint controllers.	Revised joint controller/processor agreement drafted	**Eliminated**	**Low**	**Y**
No written contract in place with data processors.	Revised joint controller/processor agreement drafted and Master Security Questionnaire to be completed	**Eliminated**	**Low**	**Y**
No BCP, recovery plan or backups in place.	Review ASC BCDR and clarify LL and Cerner backup arrangements	**Reduced**	**Low**	**Y**
Staff not adequately trained.	Clarify training arrangements, any available guidance materials etc	**Reduced**	**Low**	**Y**
Data subject requests are not responded to in required timescales	Comms to ensure ASC staff aware to signpost clients to GNCR 'opt-out' channels in addition to 'local' processes around subjects' rights	**Reduced**	**Low**	**Y**

	(note SAR and right to erasure do not apply to data in HIE)			
Data can be restricted (if applicable).	Confirm process and facility for setting relevant restrictions within HIE if objection raised; review current processes around objection/restriction to align with HIE standard operating process	**Reduced**	**Low**	**Y**
Data transferred or stored outside EU e.g. in cloud without adequate safeguards.	Clarify with Cerner Security Plan (note Brexit context for 3rd countries, international transfers)	**Reduced**	**Low**	**Y**
Backups held outside EU, without adequate safeguards.	Clarify with Cerner Security Plan (note Brexit context for 3rd countries, international transfers)	**Reduced**	**Low**	**Y**

Step 7: Sign off and record outcomes		
Item	**Name/date**	**Notes**
Measures approved by: (Head of Service)		
Residual risks approved by: (Head of Service)		
DPO advice provided:		
Summary of DPO advice:		
DPO advice accepted or overruled by: (Head of Service)		If overruled, you must explain your reasons
Consultation responses reviewed by:	Not applicable	If your decision departs from individuals' views, you must explain your reasons
Comments:		
This DPIA will kept under review by:		The DPO should also review ongoing compliance with DPIA