Data Protection Impact Assessment (DPIA)

Guidance

What you need to consider and how to complete the SCW Template

Contents

Key Legislation and Codes of Practice

You should be aware of the Data Protection Legislation that govern how organisations must safeguard information, what processes should be in place to use, secure and transfer information and also how patients and members of public can exercise their rights under that legislation. This area is complex but can be viewed as follows.

Data Protection Legislation can be used as a generic term which encompasses the following:

- the Data Protection Act 2018 (DPA 2018)
- the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679),
- the Law Enforcement Directive (LED) (Directive (EU) 2016/680) (only applicable to certain organisations)
- regulations made under the DPA 2018
- any applicable national Laws implementing them as amended from time to time
- all applicable Law concerning privacy, confidentiality or the processing of personal data including but not limited to the Human Rights Act 1998, the Health and Social Care (Safety and Quality) Act 2015, the common law duty of confidentiality and the Privacy and Electronic Communications (EC Directive) Regulations

In addition, organisations must take account of the following as part of their information governance and management practices (where applicable):

- Freedom of Information Act 2000
- Environmental Information Regulations
- INSPIRE Regulations
- Health and Social Care Act 2012
- Access to Health Records Act 1990
- Public Records Act 1958
- Mental Capacity Act 2005
- Computer Misuse Act 1990
- Copyright, Designs and Patents Act 1988

The organisation must also have regard for the following standards and Codes of Practice (where applicable):

- International information security standard: ISO/IEC 27002: 2005
- Caldicott Principles
- Data Security and Protection Toolkit
- Data and cyber security: protecting information and data in health and care
- Data Sharing - Data Protection Code of Practice - ICO
- Codes of practice for handling information in health and care
    - Records Management Code of Practice for Health and Social Care
    - Code of practice on confidential information
    - HSCIC Guide to Confidentiality
    - Confidentiality
    - Information security management NHS code of practice
    - NHS Information Governance - Guidance on Legal and Professional Obligations
- Confidentiality Supplementary Guidance - Public interest disclosures
- CCTV
- Privacy notices, transparency and control
- ICO guidance - Anonymisation
- Personal Information Online Code of Practice

Abbreviations and Meanings

Often abbreviations are used and listed below are a number of them you may come across whilst reading this guidance. You may wish to add your own.

Abbreviation	Meaning
BCM	Business Continuity Management
BCP	Business Continuity Plan
BOB ICB	Buckinghamshire, Oxfordshire and Berkshire West Integrated Care Board
CSU	Commissioning Support Unit
DC	Data Custodian
DPA	Data Processing Agreement
DPA 2018	Data Protection Act 2018
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
DSA	Data Sharing Agreement
e-LfH	E learning for health (online training provider)
FOI/FOIA	Freedom of Information Act 2000
FPN	Fair Processing Notification (privacy notice)
GDPR	General Data Protection Regulation
GP	General Practitioner
IAA	Information Asset Administrator (interchangeable term for Data Custodian)
IAO	Information Asset Owner
ICO	Information Commissioners Office
IG	Information Governance
IT	Information Technology
SCW	South, Central and West
SIRO	Senior Information Risk Owner

The Template

This template is for use where you are acting as a Controller or have been asked to undertake a DPIA on behalf of other Controllers. You can of course use it in any circumstances where you wish to determine if you have embedded the principles of data protection by design and default.

A DPIA should begin early in the life of a project, before processing starts, and run alongside the planning and development process. Responsibility for the DPIA lies with the project lead or manager, someone with the authority over the project to effect change. The lead and author may not necessarily be the same person. The project lead and author details are entered on page 2 of the template.

The Data Protection Officer can advise on the completion of a DPIA.

The template includes fields that enable you to input text and other information such as dates and drop down menu selections. The majority of the template is locked meaning that the response fields cannot be deleted. Should you wish to alter or delete a previously entered response then please just delete the text which should make the instruction 'click here to enter text/a date' to reappear. If changing a check box selection, clicking on the box will add a tick, a second click will remove the tick. If changing or deleting an option from a drop down selection then simply reselect the 'Choose an item' field to remove any other text. You cannot add text of your own choosing to any field except those indicated by 'click here to enter text' instructions.

Your first task is to determine if you need to do a DPIA or should consider doing one if not a legal obligation. Page 1 of the template asks you to consider a series of statements and tick if you believe the existing or proposed processing of data to fits any of those statements. Tick the ones that do and leave those that don't as an empty square (note if you tick the square will disappear).

We will now move on to the template and the expected responses.

Background Information	
Date of your DPIA :	Select the date from the calendar option by clicking the mouse anywhere over the words [Click here to enter a date] and then selecting the button to choose the date you want. It can be the date you are writing it, reviewing it or submitting it, this is up to you.
Title of the activity/processing:	Click here to enter text. Call it what is most meaningful to you.
Who is the person leading this work?	Click here to enter text. Name the most appropriate person.
Who is the Lead Organisation?	Click here to enter text. Identify the lead for the DPIA work.
Who has prepared this DPIA?	Click here to enter text. Who are you?.
Who is your Data Protection Officer?	Click here to enter text. Name the DPO you would discuss this DPIA with.
Describe what you are proposing to do:	Click here to enter text. Include as much background information as you can about why the new system/change in system/sharing of information/data processing is required.
Are there multiple organisations involved?	Click here to enter text. You can use this space to name them, and who their key contact for this work is but put not applicable if just one organisation**.**
Can you think of any other Key Stakeholders that should be consulted or involved in this DPIA?	Click here to enter text. Identify anyone or organisation that you feel may add understanding to what you are assessing or who may be affected by the outcome/s.
Detail anything similar that has been undertaken before?	Click here to enter text. If you know that another organisation has undertaken this activity or something similar then please detail along with the dates. Include the similarities or differences between your activity and any undertaken previously. Examples could include ✓ Prior DPIAs on similar projects, whether conducted within the organisations, or by other organisations or in other countries. ✓ Fact sheets, white papers, reports and refereed articles published by industry associations, technology providers, and research centres. ✓ Consultations with professional associations. Possibilities include Department of Health and NHS England but the orientation and expertise of organisations like these may vary over time. ✓ Consultations with other regulators. ✓ Consultations with non-government organisations that represent or provide advice to those potentially affected by the project.

Categories of data

1.1 What data/information will be used?

Tick the available box or leave blank. To help you:

Description of the categories and examples
Personal Data Any one piece of information or combination of information relating to an identified or identifiable person who can be directly or indirectly identified by that information e.g. 1) Name; 2) an identification number e.g. NHS number, hospital number, NI number, passport number, driving licence number etc.; 3) location data e.g. address, postcode, place of work, GIS maps or application location data; 4) an online identifier e.g. IP address or cookie identifier, social media username, e-mail address or 5) 5. factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of a person
Special Categories of Personal Data (a) The racial or ethnic origin of the data subject (b) Their political opinions (c) Their religious beliefs or other beliefs of a similar nature (d) Whether a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1998 (e) Genetic data (f) Biometric data for the purpose of uniquely identifying a natural person (g) Their physical or mental health or condition (h) Their sexual life
Personal Confidential Data Personal and Special Categories of Personal Data owed a duty of confidentiality (under the common law). This term describes personal information about identified or identifiable individuals, which should be kept private or secret and could be considered 'sensitive' in nature. The definition includes dead* as well as living people and 'confidential' includes information 'given in confidence' and 'that which is owed a duty of confidence'. **The term is used in the Caldicott 2 Review: Information: to share or not to share (published March 2013)*
Sensitive Data (GDPR definition Article 10) Information concerning law enforcement activities or that processed by the Intelligence Services.
Pseudonymised Data Pseudonymisation is a technique that replaces or removes information in a data set that identifies an individual. The GDPR defines pseudonymisation as: "…the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person." Pseudonymisation may involve replacing names or other identifiers which are easily attributed to individuals with, for example, a reference number. Whilst you can tie that reference number back to the individual if you have access to the relevant information, you put technical and organisational measures in place to

ensure that this additional information is held separately.

Pseudonymising personal data can reduce the risks to the data subjects and help you meet your data protection obligations.

However, pseudonymisation is effectively only a security measure. It does not change the status of the data as personal data.

"…Personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information, should be considered to be information on an identifiable natural person…"

Anonymised Data

The GDPR does not apply to personal data that has been anonymised. "…The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. This Regulation does not therefore concern the processing of such anonymous information, including for statistical or research purposes."

This means that personal data that has been anonymised is not subject to the GDPR. Anonymisation can therefore be a method of limiting your risk and a benefit to data subjects too. Anonymising data wherever possible is therefore encouraged.

However, you should exercise caution when attempting to anonymise personal data. Organisations frequently refer to personal data sets as having been 'anonymised' when, in fact, this is not the case. You should therefore ensure that any treatments or approaches you take truly anonymise personal data. There is a clear risk that you may disregard the terms of the GDPR in the mistaken belief that you are not processing personal data.

In order to be truly anonymised under the GDPR, you must strip personal data of sufficient elements that mean the individual can no longer be identified. However, if you could at any point use any reasonably available means to re-identify the individuals to which the data refers, that data will not have been effectively anonymised but will have merely been pseudonymised. This means that despite your attempt at anonymisation you will continue to be processing personal data.

You should also note that when you do anonymise personal data, you are still processing the data at that point.

Commercially Confidential Information

Business/Commercial information, including that subject to statutory or regulatory obligations, which may be damaging to the organisation or a commercial partner if improperly accessed or shared. Also as defined in the Freedom of Information Act 2000 and the Environmental Information Regulations.

Other

Information concerning a 'legal' rather than a 'natural' person is not personal data. Consequently, information about a limited company or another legal entity, which might have a legal personality separate to its owners or directors, does not constitute personal data and does not fall within the scope of the GDPR. Similarly, information on a public authority is not personal data.

However, the GDPR does apply to personal data relating to individuals acting as sole traders, employees, partners, and company directors wherever they are individually identifiable and the information relates to them as an individual rather than as the representative of a legal person.

A name and a corporate email address clearly relate to a particular individual and is therefore personal data. However, the content of any email using those details will not automatically be personal data unless it includes information which reveals something about that individual, or has an impact on them.

Legal Basis

1.2
Processing has to be lawful so identify which of the following you believe justifies what you are proposing to do and include an explanation as to why in the relevant box. You must select at least one from a – f.

Tick the available boxes or leave blank.

Article 6 (1) of the GDPR includes the following:

a) THE DATA SUBJECT HAS GIVEN CONSENT ☐

Why are you relying on consent from the data subject?

Click here to enter text.

Explain why no other legal basis is sufficient. To help you:

The GDPR sets a high standard for consent. Consent means offering individuals real choice and control. Genuine consent should put individuals in charge.

- ✓ Consent requires a positive opt-in.
- ✓ Explicit consent requires a very clear and specific statement of consent.
- ✓ Consent requests must be kept separate from other terms and conditions.
- ✓ Consent must be specific and 'granular' i.e. separate consent for separate things.
- ✓ It must be easy for people to withdraw consent and told how.
- ✓ Evidence of consent must be kept – who, when, how, and what.
- ✓ Consent must be kept under review, and refreshed if anything changes.
- ✓ Public authorities and employers will need to take extra care to show that consent is freely given, and should avoid over-reliance on consent.
- × Don't use pre-ticked boxes or any other method of default consent.
- × Vague or blanket consent is not enough.
- × Consent to processing must not be a precondition of a service.

Why is consent important?

Consent is one lawful basis for processing, and explicit consent can also legitimise use of special category data. Consent may also be relevant where the individual has exercised their right to restriction, and explicit consent can legitimise automated decision-making and overseas transfers of data. Relying on inappropriate or invalid consent could destroy trust and harm reputations – and may lead to large fines.

When is consent appropriate?

Consent is one lawful basis for processing, but there are alternatives. Consent is not inherently better or more important than these alternatives. If consent is difficult, consider using an alternative. If personal data would still be processed without consent, asking for consent is misleading and inherently unfair. If you still believe that consent is the lawful basis for your processing under the GDPR then complete 1.4 and 1.5 in addition to this section.

Further guidance can be found at ICO and consent

What is the process for obtaining and recording consent from the Data Subject?

Click here to enter text.

Explain the development of the consent process and importantly the consent form. This is the form that contains the 'How, where, when, by whom' statements and should ideally have similar information in it to your Fair Processing Notice. You could include your proposed consent form here or a link to it and check it against the checklist below?

Describe how your consent form is compliant with the Data Protection requirements?

Click here to enter text.

You can use this checklist to help you.

Consent guidance and checklist March 2

b) IT IS NECESSARY FOR THE PERFORMANCE OF A CONTRACT TO WHICH THE DATA SUBJECT IS PARTY ☐

Click here to enter text.

Describe the contract. Note that an NHS standard contract is unlikely to be used with an 'individual', it is more likely to be used with a provider organisation or other situation where a service is being commissioned. If the organisation is directly contracting with an individual e.g. a contract of employment then this can be relied upon as a lawful basis.

You can rely on this lawful basis if you need to process someone's personal data:

- to fulfil your contractual obligations to them; or
- because they have asked you to do something before entering into a contract (e.g. provide a quote)

The processing must be necessary. If you could reasonably do what they want without processing their personal data, this basis will not apply. You should document your decision to rely on this lawful basis and ensure that you can justify your reasoning.

When is the lawful basis for contracts likely to apply?

- ✓ you have a contract with the individual and you need to process their personal data to comply with your obligations under the contract
- ✓ you haven't yet got a contract with the individual, but they have asked you to do something as a first step (e.g. provide a quote) and you need to process their personal data to do what they ask
- × it does not apply if you need to process one person's details but the contract is with someone else
- × it does not apply if you take pre-contractual steps on your own initiative or at the request of a third party

A contract does not have to be a formal signed document, or even written down, as long as there is an agreement which meets the requirements of contract law. Broadly speaking, this means that the terms have been offered and accepted, you both intend them to be legally binding, and there is an element of exchange (usually an exchange of goods or services for money, but this can be anything of value).

When is processing 'necessary' for a contract?

The processing must be necessary to deliver your side of the contract with this particular person. If the processing is only necessary to maintain your business model more generally, this lawful basis will not apply and you should consider another lawful basis, such as legitimate interests.

What else should be considered?

If the processing is necessary for a contract with the individual, processing is lawful on this basis and you do not need to get separate consent. If processing of special category data is necessary for the contract, you also need to identify a separate condition for processing this data. If the contract is with a child under 18, you need to consider whether they have the necessary competence to enter into a contract. If you have doubts about their competence, you may wish to consider an alternative basis such as legitimate interests, which can help you to demonstrate that the child's rights and interests are properly considered and protected.

Further guidance can be found at ICO contracts

c) IT IS NECESSARY UNDER A LEGAL OBLIGATION TO WHICH THE CONTROLLER IS SUBJECT ☐

Click here to enter text.

Identify the legislation or legal obligation you believe requires you to undertake this processing. This can be

used only when you are **obliged** to process the personal data to comply with the law. It differs from Article 6 1 (e).

The legal obligation must be laid down by UK or EU law. This does not have to be an explicit statutory obligation, as long as the application of the law is foreseeable to those individuals subject to it. It includes clear common law obligations.

This does not mean that there must be a legal obligation specifically requiring the specific processing activity. The point is that your overall purpose must be to comply with a legal obligation which has a sufficiently clear basis in either common law or statute.

You should be able to identify the obligation in question, either by reference to the specific legal provision or else by pointing to an appropriate source of advice or guidance that sets it out clearly. For example, you can refer to a government website or to industry guidance that explains generally applicable legal obligations.

- Example

An employer needs to process personal data to comply with its legal obligation to disclose employee salary details to HMRC. The employer can point to the HMRC website where the requirements are set out to demonstrate this obligation. In this situation it is not necessary to cite each specific piece of legislation.

- Example

A court order may require you to process personal data for a particular purpose and this also qualifies as a legal obligation. Regulatory requirements also qualify as a legal obligation for these purposes where there is a statutory basis underpinning the regulatory regime and which requires regulated organisations to comply.

When is processing 'necessary' for compliance?

Although the processing need not be essential for you to comply with the legal obligation, it must be a reasonable and proportionate way of achieving compliance. You cannot rely on this lawful basis if you have discretion over whether to process the personal data, or if there is another reasonable way to comply. It is likely to be clear from the law in question whether the processing is actually necessary for compliance.

What else should be considered?

If you are processing on the basis of legal obligation, the individual has no right to erasure, right to data portability, or right to object.

For further guidance go to ICO legal obligation

d) IT IS NECESSARY TO PROTECT THE VITAL INTERESTS OF THE DATA SUBJECT OR ANOTHER NATURAL PERSON ☐

Click here to enter text.

Explain why you have chosen this. Vital interests are intended to cover only interests that are essential for someone's life. So this lawful basis is very limited in its scope, and generally only applies to matters of life and death.

It is likely to be particularly relevant for emergency medical care, when you need to process personal data for medical purposes but the individual is incapable of giving consent to the processing.

- Example

An individual is admitted to the A & E department of a hospital with life-threatening injuries following a serious road accident. The disclosure to the hospital of the individual's medical history is necessary in order to protect his/her vital interests.

It is less likely to be appropriate for medical care that is planned in advance. Another lawful basis such as public task or legitimate interests is likely to be more appropriate in this case.

It may also be relevant, for example, if it is necessary to process a parent's personal data to protect the vital interests of a child.

Vital interests are also less likely to be the appropriate basis for processing on a larger scale.

For further information go to ICO vital interests

e) IT IS NECESSARY FOR THE PERFORMANCE OF A TASK CARRIED OUT IN THE PUBLIC INTEREST OR UNDER OFFICIAL AUTHORITY VESTED IN THE CONTROLLER ☐

Click here to enter text.

Can be used where processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Controller. This can be laid down by law; or in the exercising of official authority (for example, a public body's tasks, functions, duties or powers) which is laid down by law. This is the most common condition for processing used within the health sector.

If you can show you are exercising official authority, including use of discretionary powers, there is no additional public interest test. However, you must be able to demonstrate that the processing is 'necessary' for that purpose. 'Necessary' means that the processing must be a targeted and proportionate way of achieving your purpose. You do not have a lawful basis for processing if there is another reasonable and less intrusive way to achieve the same result.

What does 'laid down by law' mean?

The relevant task or authority must be laid down by domestic or EU law. This will most often be a statutory function. However, this does not have to be an explicit statutory provision, as long as the application of the law is clear and foreseeable. This means that it includes clear common law tasks, functions or powers as well as those set out in statute or statutory guidance. You do not need specific legal authority for the particular processing activity. The point is that your overall purpose must be to perform a public interest task or exercise official authority and that overall task or authority has a sufficiently clear basis in law.

Who can rely on this basis?

Any organisation exercising official authority or carrying out a specific task in the public interest. The focus is on the nature of the function, not the nature of the organisation.

❖ Example

Private water companies are likely to be able to rely on the public task basis even if they do not fall within the definition of a public authority in the Data Protection Act 2018. This is because they are considered to be carrying out functions of public administration and they exercise special legal powers to carry out utility services in the public interest.

When can we rely on this basis?

Section 8 of the Data Protection Act 2018 (DPA 2018) says that the public task basis will cover processing necessary for:

- ✓ the administration of justice;
- ✓ parliamentary functions;
- ✓ statutory functions;
- ✓ governmental functions; or
- ✓ activities that support or promote democratic engagement

If you have other official non-statutory functions or public interest tasks you can still rely on the public task basis, as long as the underlying legal basis for that function or task is clear and foreseeable.

For accountability purposes, you should be able to specify the relevant task, function or power, and identify its basis in common law or statute. You should also ensure that you can demonstrate there is no other

reasonable and less intrusive means to achieve your purpose.

What else should be considered?

Individuals' rights to erasure and data portability do not apply if you are processing on the basis of public task. However, individuals do have a right to object. You should consider an alternative lawful basis if you are not confident that processing is necessary for a relevant task, function or power which is clearly set out in law. Remember that the GDPR specifically says that further processing for certain purposes should be considered to be compatible with your original purpose. This means that if you originally processed the personal data for a relevant task or function, you do not need a separate lawful basis for any further processing. If you are processing special category data, you also need to identify an additional condition for processing this type of data. The Data Protection Act 2018 includes specific conditions for parliamentary, statutory or governmental functions in the substantial public interest.

Further guidance can be found at

ICO Public Task

NHS Digital IGA guidance

f) IT IS NECESSARY FOR THE LEGITIMATE INTERESTS OF THE CONTROLLER OR THIRD PARTY. ☐

Click here to enter text.

Make sure that this is applicable to your organisation and is a lawful basis for processing. It can be used where:

"Processing is necessary for the purposes of the legitimate interests pursued by the Controller or by a third party except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child."

This can be broken down into a three-part test:

- Purpose test: are you pursuing a legitimate interest?
- Necessity test: is the processing necessary for that purpose?
- Balancing test: do the individual's interests override the legitimate interest?

If you are a public authority, you cannot rely on legitimate interests for any processing you do to perform your tasks as a public authority. However, if you have other legitimate purposes outside the scope of your tasks as a public authority, you can consider legitimate interests where appropriate. This will be particularly relevant for public authorities with commercial interests.

A legitimate interest is most likely to be an appropriate basis where you use data in ways that people would reasonably expect and that have a minimal privacy impact. Where there is an impact on individuals, it may still apply if you can show there is an even more compelling benefit to the processing and the impact is justified. You can rely on legitimate interests for marketing activities if you can show that how you use people's data is proportionate, has a minimal privacy impact, and people would not be surprised or likely to object – but only if you don't need consent under the Privacy and Electronic Communications Regulations (PECR). You can consider legitimate interests for processing children's data, but you must take extra care to make sure their interests are protected.

Further information if required can be found at ICO Legitimate Interests

1.3

Special category data is personal data which the GDPR says is more sensitive (see 1.1 above), and so needs more protection. In order to lawfully process special category data, you must identify both a lawful basis under Article 6 and a separate condition for processing special category data under Article 9. These do not have to be linked. There are ten conditions for processing special category data in the GDPR itself, but the Data Protection Act 2018 introduces additional conditions and safeguards. You must determine your condition for processing

special category data before you begin this processing under the GDPR and you should document it.

This can be a complex area and you are advised to seek guidance from your DPO in completing this part. Further guidance to help you independently can be found at

ICO Special Categories of data

NHS Digital IGA guidance

Article 9 (2) conditions are as follows:	Tick the available boxes or leave blank.
a) **THE DATA SUBJECT HAS GIVEN EXPLICIT CONSENT** see 1.2 a) above	☐
b) **FOR THE PURPOSES OF EMPLOYMENT, SOCIAL SECURITY OR SOCIAL PROTECTION** see 1.2 c) above	☐
c) **IT IS NECESSARY TO PROTECT THE VITAL INTERESTS OF THE DATA SUBJECT OR ANOTHER NATURAL PERSON WHERE THEY ARE PHYSICALLY OR LEGALLY INCAPABLE OF GIVING CONSENT** - see 1.2 d) above	☐
d) It is necessary for the operations of a not-for-profit organisation such as political, philosophical, trade union and religious body in relation to its members	*NA*
e) The data has been made public by the data subject	*NA*
f) For legal claims or courts operating in their judicial category	*NA*
These conditions are not applicable and therefore should not be selected.	
g) SUBSTANTIAL PUBLIC INTEREST	☐
h) PROCESSING IS NECESSARY FOR THE PURPOSES OF PREVENTIVE OR OCCUPATIONAL MEDICINE, FOR THE ASSESSMENT OF THE WORKING CAPACITY OF THE EMPLOYEE, MEDICAL DIAGNOSIS, THE PROVISION OF HEALTH OR SOCIAL CARE OR TREATMENT OR THE MANAGEMENT OF HEALTH OR SOCIAL CARE SYSTEMS AND SERVICES ON THE BASIS OF UNION OR MEMBER STATE LAW OR PURSUANT TO CONTRACT WITH A HEALTH PROFESSIONAL AND SUBJECT TO CONDITIONS AND SAFEGUARDS	☐
i) PROCESSING IS NECESSARY FOR REASONS OF PUBLIC INTEREST IN THE AREA OF PUBLIC HEALTH, SUCH AS PROTECTING AGAINST SERIOUS CROSS-BORDER THREATS TO HEALTH OR ENSURING HIGH STANDARDS OF QUALITY AND SAFETY OF HEALTH CARE AND OF MEDICINAL PRODUCTS OR MEDICAL DEVICES, ON THE BASIS OF UNION OR MEMBER STATE LAW WHICH PROVIDES FOR SUITABLE AND SPECIFIC MEASURES TO SAFEGUARD THE RIGHTS AND FREEDOMS OF THE DATA SUBJECT, IN PARTICULAR PROFESSIONAL SECRECY	☐
j) PROCESSING IS NECESSARY FOR ARCHIVING PURPOSES IN THE PUBLIC INTEREST, SCIENTIFIC OR HISTORICAL RESEARCH PURPOSES OR STATISTICAL PURPOSES IN ACCORDANCE WITH ARTICLE 89(1) BASED ON UNION OR MEMBER STATE LAW WHICH SHALL BE PROPORTIONATE TO THE AIM PURSUED, RESPECT THE ESSENCE OF THE RIGHT TO DATA PROTECTION AND PROVIDE FOR SUITABLE AND SPECIFIC MEASURES TO SAFEGUARD THE FUNDAMENTAL RIGHTS AND THE INTERESTS OF THE DATA SUBJECT.	☐

Responsibility

1.4

Confirm who the Controller and Processor is/are. Confirm if the Controller/s are solely or jointly responsible for any data processed?

Name of Organisation	Role
Click here to enter text.	Choose an item.
Click here to enter text.	Choose an item.

List the organisations that are involved and what you know or believe to be their role under Data Protection Legislation. The Role column enables you to choose this but if you do not know then leave it blank or select **Still to be confirmed'** and talk to your DPO. If you need to, copy and paste the last empty row (the entire row) in the

table to add organisations where required (the text has been left unlocked for this purpose on that row only)

To help you, a **Controller** has statutory obligations as set out by the Data Protection Legislation. A Controller determines the purposes and means of processing personal data and remains responsible for the data where a Processor is involved. A Controller can do this alone (**sole Controller**) or with others (**joint Controller**) but this is a complex area.

In general, joint Controllers have a common objective with others regarding the processing, are processing the personal data for the same purpose as another controller, are using the same set of personal data (e.g. one database) for this processing as another controller, have designed this process with another controller and have common information management rules with another controller.

Whenever a Controller uses a **Processor** it needs to have a written contract/agreement in place so that the parties understand their responsibilities and liabilities. The GDPR places further obligations to ensure contracts with Processors comply with the GDPR. Controllers are liable for their compliance with the GDPR and must only appoint Processors who can provide 'sufficient guarantees' that the requirements of the GDPR will be met and the rights of data subjects protected. It is important to understand who else may be involved in the project/activity in order to understand the relationships to the data/information that will need to be reflected in accompanying agreements.

Processing

1.5

Describe exactly what is being processed, why you want to process it and who will do any of the processing?

Click here to enter text.

Consider what it is you plan to process and why you want to do this. What are your intended outcomes? What are your interests in the outcomes? What benefits are there for the organisations involved or for society as a whole? Who is going to do the processing is it you or someone else?

Confidentiality

1.6

Tick here if you owe a duty of confidentiality to any information ☐

If so, specify what types of information

Click here to enter text.

List the type of information that you feel falls into this category.

What is the Duty of Confidentiality?

- A duty of confidence arises when one person discloses information to another (e.g. patient to clinician) in circumstances where it is reasonable to expect that the information will be held in confidence and is a legal obligation that is derived from case law;
- is a requirement established within professional codes of conduct; and
- must be included within NHS employment contracts as a specific requirement linked to disciplinary procedures

Patients entrust the NHS with information relating to their health and other matters as part of their seeking treatment. They do so in confidence and they have the legitimate expectation that staff will respect their privacy and act appropriately. In some circumstances patients may lack the competence to extend this trust, or may be unconscious, but this does not diminish the duty of confidence. It is essential, if the legal requirements are to be met and the trust of patients is to be retained, that the NHS provides, and is seen to provide, a confidential service.

Information that can identify individual patients must not be used or disclosed for purposes other than direct care without the individual's consent (ideally explicit), some other legal basis, or where there is a robust public

interest or legal justification to do so. In contrast, anonymised information is not confidential and may be used with relatively few constraints. Information that has been pseudonymised may be disclosed in controlled circumstances, such as where receiving organisations have no way to re-identify the individuals. As this is a complex area, always seek advice and support.

The following table may be helpful

What information?	Category of data	How was it obtained?	Is it confidential data?
Name and address and postcode	Personal Data	Electoral register	No
Full Postcode, recent hospital admissions, age, marital status	Personal Data and Special category of personal data	Performance report	Yes – measures to reduce the risk of identifying the person should be taken by reducing the postcode search criteria and where possible using age brackets
Member of local church	Special Category of Personal Data	Facebook members group post	No – made public by the individual
Religious belief limiting health care	Special Category of Personal Data	Patient to GP consultation	Yes – GP would only share if Patient would expect this for their care
Date of surgery on knee	Special Category of Personal Data	Individual posted photo of themselves in hospital	No – made public by the individual
Date of surgery on knee	Special Category of Personal Data	GP included in request for further funding for additional operation	Yes – GP would only share if Patient would expect this for their care
Sexual orientation	Special Category of Personal Data	Identifies own orientation on social media or other public forum	No – made public by the individual
Sexual orientation	Special Category of Personal Data	Consultant includes information on orientation within hospital record	Yes – highly confidential and Consultant would only share if Patient would expect this for their care or has given explicit consent

1.7

How are you satisfying the common law duty of confidentiality?

Choose an item.

- **CAG Section 251 approval (please specify)** – This is a specific granting of permission to use confidential data without the consent of the individual. Approval is gained by application to the Confidentiality Advisory Group (CAG) of the Health Research Authority and granted under powers of section 251 of the Health & Social Care Act 2006. Applications are usually made where a project is unable to justify the processing of confidential data via any of the other options, or where there is a public interest, but it is debatable how substantial that is.
- **Consent (explicit)** – where individuals are specifically informed about the use of their data and asked to confirm that they consent to its use, either verbally or in writing (NB this can cause confusion with the lawful basis for processing under data protection legislation – seek advice if using this option)
- **Consent (implied)** – where individuals are informed, ideally specifically, that their data is to be used and what for and have not raised any concern or objection

- **Legal duty (please specify)** – Where in the circumstances there is a duty set out in legislation applicable to the organization/s to use/share the data, i.e. to share serious safeguarding concerns for a child.
- **No disclosure of confidential data takes place** – For the common law duty of confidentiality to be engaged there has to be a disclosure (or potential) of the data. Disclosure is generally where the information is accessed or shared with another person. Disclosure does not take place if:
  - The processing is done by automated systems and not visible to a person (i.e. automated processes to remove identifiers to either anonymise or pseudonymise the data.
  - Someone with justifiable access to the confidential data undertakes to anonymise/pseudonymised the data prior to disclosure to another party
- **Reasonable expectation (please specify)** – where in all circumstances is it reasonable to expect an individual to understand without specifically informing them that their data will be used in this way, i.e. recording the view of the patient during a consultation or sending a referral from general practice to hospital outpatients that the patient has requested.
- **Substantial Public interest (please specify)** – Where there isn't a legal duty (see above), but the use/sharing of data is crucial to supporting a wider, robust public interest. This is more often used on a case by case basis and would not often apply to general processing of data. An example can be the sharing of data on vulnerable adults where abuse is suspected (which isn't bound by the same legal duty as for children).

If you have selected an option which asks for further information please enter it here

Click here to enter text.
Describe why you have chosen this option.

1.8

Are you applying any anonymisation/pseudonymisation technique or encryption to any of the data to preserve the confidentiality of any information?

Choose an item.
Select **yes, no or don't know**. If you don't know then please find this information out as there are potential privacy implications with the processing.

If you are then describe what you are doing.

Click here to enter text.
Describe what the organisation is doing or what another organisation is doing or already has done. To help you, The Anonymisation Code of Practice issued by the ICO is a comprehensive guidance document that attempts to explain this very complex and technical area.

Purpose

1.9

Tick here if you are intending to use any information for a purpose that isn't considered as direct patient care. ☐

If so describe that purpose.

Click here to enter text.
Describe any circumstances where, for example, the processing of data for direct care purposes is then used for analysis, research or another purpose. To help you, **Direct Care** is defined as

"A clinical, social or public health activity concerned with the **prevention, investigation and treatment of illness** and the alleviation of suffering of **individuals.** It includes supporting **individuals'** ability to function and improve their participation in life and society. It includes the assurance of safe and high quality care and treatment through local audit, the management of untoward or adverse incidents, person satisfaction including

measurement of outcomes undertaken by one or more registered and regulated health or social care professionals and their team with whom the individual has a legitimate relationship for their care".

Secondary uses means using data for the purposes of planning, agreeing and monitoring health services. It is not one action but many, ranging from the health-needs assessment for a population, through the clinically based design of patient pathways, to service specification and contract negotiation or procurement, with continuous quality assessment.

The Data Services for Commissioners programme has been established to improve NHS commissioning by ensuring that commissioning decisions, and the insights that support them, are based upon robust, standardised data that has been processed efficiently and is accessed legally. For the purposes of this programme, NHS Digital collects the personal data from the organisations that provide health care which includes information about the diagnosis, treatment received, postcode and date of birth. It also includes NHS number which is used by NHS Digital to link data from several sources. NHS Digital provides data that is pseudonymised in accordance with the Information Commissioner's Anonymisation code of practice which is then used for commissioning purposes. This data is used by Clinical Commissioning Groups and is obtained through the local NHS Digital office usually known as the DSCRO (Data Services for Commissioners Regional Office).

1.10
Approximately how many people will be the subject of the processing?

Choose an item.
A number of possible responses are included for you but there is no exact science in this. Try and assess the numbers involved even if they are approximations e.g. GP patients in Coastal West Sussex CCG area = 515,000, Somerset CCG = 575,000, BNSSG CCGS = 1,009,500. If you do not know then use one of the generic population responses.

Collection and Use

1.11
How are you collecting the data?

Choose an item.
Choose an item.
Choose an item.
Choose an item.
Choose an item.

If you have selected 'other method not listed' describe what that method is.
Click here to enter text.

This should be self-explanatory and if you need to add more selections then copy the last 'choose an item' and paste, the text has been left unlocked for you to do this.

It is important to capture the method of collecting for any types of data, a verbal transaction may then become a written transaction, on paper or electronic and it is important to consider the ways that social media and online services may capture data as part of the service.

1.12
How will you edit the data?

Click here to enter text.
Your response will depend upon the activity proposed. If you are implementing a new software solution or collecting data/information for the first time then you need to consider who is responsible for the editing and deletion of records. This is likely to be the organisation responsible for the records i.e. the Controller or the Processor where another organisation is asked to undertake these activities. You may need to speak to whoever is providing the service to find this information out.

1.13
How will you quality check the data?

Click here to enter text.
Your response will depend upon the activity proposed. If you are implementing a new software solution or collecting data/information for the first time then you need to consider who is responsible for the quality of the records. This is likely to be the organisation responsible for the records i.e. the Controller or the Processor where another organisation is asked to undertake these activities. You may need to speak to whoever is providing the service to find this information out.

1.14
Review your business continuity or contingency plans to include this activity.

Each organisation should have plans in place to identify the risks to data/information if affected by issues such as power outage, loss of access to data/information, loss of access to buildings etc. A business continuity plan or other such document should be in place to identify where this could occur and what steps should be taken to mitigate such risks.

Have you identified any risks?

Choose an item.
Select **yes, no or don't know**. If you don't know then please talk to the person responsible for this in your service area. This risk assessment may also be part of the Information Asset Register for which this activity relates to.

If yes is selected, include in the risk section of this template.

1.15
What training is planned to support this activity?

Click here to enter text.
Your response will depend upon the activity proposed. Additional training may be required in order to help staff understand their responsibilities with respect to the proposed activity and the information involved. This could include additional Information Governance training, records management training, training on proposed operating procedures or training to use a new software system.

Linkage

2.1
Are you proposing to combine any data sets?

Choose an item.
Select **yes, no or don't know**. If you don't know then please talk to the person responsible for undertaking the data landing and analysis.

If yes then provide the details here.

Click here to enter text.
In order to achieve the proposed activity you may wish to combine existing or new datasets and as each dataset may be subject to differing rules on their use it is essential that any proposed linkages are identified very early in the planning process. This is particularly important if you are intending to use any of the data/information gathered as part of the proposed activity for a purpose other than the primary one. For example, you may wish to collect data/information for the purposes of Direct Patient Care but then be able to use all or part of the data to evaluate the service provided or gain feedback from the Patients who will be involved in the proposed activity.

Another example may be that you wish to commission a different service but in order to obtain source data to base your planning assumptions on, you need data/information from different sources e.g. GP's, Acute hospital

providers and community providers. Again you will need to consider how you can use these data sets in a way that does not breach the Data Protection Legislation.

Data flows

2.2
What are the Data Flows?

Click here to enter text.
It is important to establish ALL data flows and data linkages as part of the DPIA. A diagram explaining the sources of data, the flows (inbound and outbound) and all of the organisations involved is essential in determining the different risks and issues that could arise as a result of your proposed activity. You may have it already prepared in a tabular form or can produce a simple line drawing or flow chart, as long as it includes all of the proposed flows, sources and organisations. Attach it to the DPIA or include as an embedded document in the template.

Sharing and National Data Opt Out

2.3
What data/information are you planning to share?

Click here to enter text.
This is a very important question for a variety of reasons. Describe what you are planning to share down to individual data item level e.g. NHS number, Patient name, condition, e-mail address, GP Practice code etc.

2.4
Is any of the data subject to the National Data Opt Out?

Choose an item.
Select **yes, no or don't know**.

There is comprehensive guidance on National data opt out

If your organisation has to apply it describe the agreed approach to this

Click here to enter text.

If another organisation has applied it add their details and identify what data it has been applied to

Click here to enter text.

If you do not know if it applies to any of the data involved then you need to speak to your Data Protection Officer to ensure this is assessed.

2.5
Who are you planning to share the data/information with?

Click here to enter text.
This is a very important question for a variety of reasons. Different organisations have different roles and responsibilities and therefore you must identify all of the partners e.g. GP records are collected for the purpose of the delivery of primary care services to a Patient. The data may then need to be shared with a community provider by way of a referral for further care. The data may also need to be shared for other purposes such as invoice validation or payment or for other support services not classed as Direct Patient Care.

2.6
Why is this data/information being shared?

Click here to enter text.
Again this relates to the purpose and legal basis for doing so. You may intend to ask for a number of data items to be collected (as above) but you must always be aware of why another person/organisation should receive the

data – the purpose must be explicitly specified.

2.7
How will you share it?

Click here to enter text.
In order to ensure that data/information is processed in accordance with the Data Protection Legislation you must identify how it will be shared. Will you use an electronic method, text services or ask someone to log into an online system or survey facility? Will you ask someone to produce a report and then send it by post? All methods for sharing data must be safe and not introduce risk of data loss or inappropriate access.

Tick if you are planning to use Microsoft Teams or another similar online networking/meeting solution that may have the facility to store or record conversations or related data as part of the sharing arrangements
☐

Provide details of how you have considered any privacy risks of using one of these solutions

Click here to enter text.
If you are using Microsoft Teams, are you certain that any information shared through that platform is done so securely, is that data stored? Will the picture of a Patients X-ray or test results be stored in the cloud somewhere that you are not aware of? You should seek advice from the IT team that is installing or making the solution available to you to check that all of these things have been considered alongside having a standard operating procedure or set of rules in place to make sure information remains safe and secure.

Sharing agreements

2.8
What data sharing agreements are or will be in place?

Click here to enter text.
In addition to a contract and/or a Data Processing Agreement (DPA) it is highly recommended that you put in place a further agreement called a Data Sharing Agreement (DSA) where this is applicable. This agreement is usually between Controllers who are sharing data for a specific reason and is different from the DPA. The DSA is not a legal requirement but it does provide the means to describe all partners relationship to that shared data and will help each Controller explain to Patients and other data subjects who is seeing or using their data and why. Importantly it will set out the responsibilities of each party and is essential where joint Controller relationships exist. Most of the information needed for that agreement will be sourced from this DPIA and any relevant additional documents. Your Information Governance Lead or DPO will be able to assist you with this and support you to complete an example template document that will need to be agreed by the organisations involved and signed. It is important that this is reviewed on at least an annual basis or where a change in the proposed activity requires this if sooner.

If there is already an agreement in place then attach it to the DPIA or include as an embedded document in the template. Make sure it reflects your responsibilities and obligations if you are a Controller and if not, ask for it to be amended.

Reports

2.9
What reports will be generated from this data/information?

Click here to enter text.
If your proposed activity includes the publication or sharing of reports then you must identify how the data/information within that report is to be presented. Detail whether reports will be

A) Identifiable, i.e. you can see who the information in the report relates to,
B) pseudonymised at patient level, i.e. you will be able to see individual rows of data but the personal

identifier (usually the NHS number) will be replaced in a way that could enable further data sets to be linked to that row of data if the same pseudonymisation linkage key is used

C) anonymised at patient level, i.e. you will be able to see individual rows of data but anything which could identify an individual has been removed and so cannot be linked to any other data set or source

D) aggregated data, i.e. the data will not be produced at individual record level but aggregated or collected together to produce a table or graph presenting the findings of an analysis of the record level data

E) used for research purposes as use of data for research purposes may need to be considered by other organisations before any DPIA can be considered

NHS Digital

2.10

Are you proposing to use Data that may have come from NHS Digital?

Choose an item.

Select **yes, no or don't know**. If you don't know then please talk to the person responsible for undertaking the data landing and analysis.

If yes are all the right agreements in place?

Choose an item.

Select **yes, no or don't know**.

Click here to enter text.

If a Data Sharing Agreement is in place then you should identify the relevant agreement and provide the details here including the date it was signed and the NIC approval number.

If you don't know then please talk to the person responsible for undertaking the data landing and analysis or your DPO.

All organisations wishing to use data given to them by NHS Digital must have made an application to do so and once approved, be in receipt of a fully signed Data Sharing Agreement setting out a) the data that can be used, b) how it can be used (purpose), c) who can use it (sharing) and d) what it can be linked with (linkages).

The types of data/information that will need to considered here includes (but may not be limited to) datasets that are submitted to NHS Digital through the Secondary Use Service route for which there is a statutory obligation for it to be collected by NHS Digital. It may also include data/information that is included as a performance or contract measure as part of an NHS contract/SLA/MOU or other such agreement.

In order for data sets of this type to be used for secondary uses, an assurance process must be in place to ensure that the intended use of the data is legal and for a purpose that does not breach someone's rights under the Data Protection Legislation and is in accordance with the Health and Social Care Act 2012, Chapter 7, Part 9, Chapter 2, section 252 to 277.

As data will flow from NHS and other providers with all identifying details included, NHS Digital will, through their Data Services for Commissioners Regional Offices (DSCRO), ensure that Patient objections for use of their data in this way are honoured by removing their data from the resulting data sets. The data that remains can then be used by Commissioners and other organisations in a way that enables data sets to be linked but protects the identity of the Patient to which the data refers or for purposes where identifiable data is required such as for Risk Stratification or Invoice Validation.

Data Processor

3.1

Are you proposing to use a third party, a data processor or a commercial system supplier?

Choose an item.

Select **yes, no or don't know**.

If yes use this space to add their details including their official name and address. If there is more than one then include all organisations.
Click here to enter text.

If you don't know then stop and try and find this information out before proceeding.

A Processor is responsible for processing personal data on behalf of a Controller and must only act on the documented instructions of a Controller. The GDPR places specific legal obligations on them and they are required to maintain records of personal data and processing activities. They will have legal liability if responsible for a breach.

If a Processor uses a sub-Processor then it will, as the original Processor, remain directly liable to the Controller for the performance of the sub-Processor's obligations.

If you are commissioning a new service/IT System/provider and this has been supported through a procurement route, a number of IG and IT assurances may have been gained as part of the procurement stages.

IG Assurances

3.2
Is each organisation involved registered with the Information Commissioner? Copy and paste the last empty row in the table to add organisations where required (the text has been left unlocked for this purpose on that row only)

Name of organisation	Registered	Registration details or comments if not registered
Click here to enter text.	Choose an item.	Click here to enter text.
Click here to enter text.	Choose an item.	Click here to enter text.

You can search their registration details here ICO register of fee payers. You can copy and paste the statement into the template.

3.3
What IG assurances have been provided to you and does any contract contain IG clauses that protect you as the Controller? (e.g. in terms and conditions, their contract, their tender submission). Copy and paste the last empty row in the table to add organisations where required (the text has been left unlocked for this purpose on that row only)

Name of organisation	Brief description of assurances obtained
Click here to enter text.	Click here to enter text.
Click here to enter text.	Click here to enter text.

A checklist to help you is available.

Processor Checklist May 2018.docx

There are a number of key assurance mechanisms that can demonstrate robust IG and IT security compliance in order to protect NHS data. Alongside the NHS Digital Data Security and Protection Toolkit, there are other areas of good practice and accreditations that an organisation can adopt or obtain. Some of these are listed here:

Checklist for IT security May 2018.dc

NHS Digital cyber and data security policy and good practice
ISO/IEC 27002:2013

National Cyber Security Centre Cyber Essentials

3.4
What is the status of each organisation's Data Security Protection Toolkit?

Copy and paste the last empty row in the table to add organisations where required (the text has been left unlocked for this purpose on that row only)

Name of organisation	ODS Code	Status	Published date
Click here to enter text.	Click here to enter text.	Click here to enter text.	Click here to enter text.
Click here to enter text.	Click here to enter text.	Click here to enter text.	Click here to enter text.

For all organisations handling NHS Patient data/information or data sets that may be derived from that data/information, there is a requirement to have appropriate Information Governance Assurances in place. Many organisations are mandated to complete the NHS Digital Data Security and Protection Toolkit (previously the Information Governance Toolkit) as part of their contract. Some organisations also opt to complete this toolkit as it is a good standard to work to. You can find out if the organisations that are party to this project/activity have a published Toolkit on the **DSP Toolkit.**

Storage

3.5
How and where will the data/information be stored?

Click here to enter text.
Will it be stored electronically, paper or another storage medium? Will it be held on digital media such as disks or removable media such as USB drives or memory sticks? Will it be held on a server, other hardware or in a virtual environment? Microfiche and other archives should be considered if relevant. Where is the server, in a building, in a third party data centre, held overseas? Will physical assets be held in paper based storage, safe storage, scanned and held electronically? Will any building become vacant or not managed in the future, could it be sold? Where in any building is the information i.e. in a locked room, in the basement, in a loft? Include information about back-ups and copies and consider what you added to 2.7 above.

Access

3.6
How is the data/information accessed and how will this be controlled?

Click here to enter text.
Will the data be accessed electronically, physically or by other means? What access controls are or will be in place to ensure that the data/information is only accessed by those authorised to do so? These could be physical measures such as key codes to buildings or system measures such as role based access, passwords and appropriate 2 factor authentication implementation for electronic storage solutions.

Cloud

3.7
Is there any use of Cloud technology?

Choose an item.
Select **yes, no or don't know**

If yes add the details here.
Click here to enter text.
Include confirmation of whether they are part of the UK Government's 'Official Digital Marketplace' and if they are G-Cloud 11 Framework accredited. See here for more information Digital Market Place G Cloud Services

If you don't know then stop and try and find this information out before proceeding.

Cloud Computing is the use of multiple server computers via a digital network as if they were one. The 'Cloud' itself is a virtualisation of resources (networks, servers, applications, data storage and services) allowing on-demand access for the end user. These resources can be provided with minimal management or service provider interaction. Cloud Computing brings many benefits to the end user, including:

- ✓ access to a huge range of applications without having to download or install anything;
- ✓ the ability to access applications from any computer, anywhere in the world;
- ✓ savings on hardware and software costs as users only use what they need;
- ✓ the ability for companies to share resources in one place;
- ✓ savings as consumption is billed as a utility, with minimal upfront costs;
- ✓ scalability via on-demand resources

Risks related to Cloud Computing include:

- × Users do not physically possess storage of their own data, which leaves the responsibility and control of data storage with the provider.
- × Users could become dependent upon the Cloud Computing provider.
- × With data held externally, business continuity and disaster recovery are in the hands of the provider.
- × There are data migration issues when changing Cloud providers.
- × What happens if your Cloud provider goes out of business?

Security

3.8
What security measures will be in place to protect the data/information?

Click here to enter text.
Guidance on what security measures should be in place can be found in section 3.3 above. Where you are implementing new technology or updating that which is already in place you must be satisfied that there are no unknown or unresolvable risks with the solution that has been proposed. If you feel that there are outstanding questions as a result of a procurement exercise or you wish to get confirmation that what is being implemented or the way that it is being done will maintain the information safely and securely then you should contact the person/organisation that provides your technology or information security support and discuss this with them. You can include your findings in this section of the DPIA template.

Is a specific System Level Security Policy needed?

Choose an item.
Select **yes, no or don't know**
If yes or don't know then you need to speak to your Data Protection Officer to ensure one is put in place if needed.

The development, implementation and management of a system level security management procedure will help to demonstrate understanding of information governance risks and help to address the security and confidentiality needs of a particular system. It should contain the range of security policy and management issues relevant to a system within technical, operational and procedural security topics. "System" relates to the complete data handling solution (electronic or otherwise) of person identifiable/special categories of personal data.

It would be expected that any electronic solution for the handling of person confidential data to comply with Cyber and Data security good practice as a minimum. In addition, NHS organisations are required to comply with security management practices as set out in ISO/IEC 27001:2013. A system level security management procedure is a core component for those organisations that undertake formal accreditation processes for their information assets.

Where a system is available to multiple organisations, the system level security management procedure must

establish the common policy, security parameters and operational framework for that system's expected operation including any functional limitations or data constraints applicable to one or more bodies.

Non-UK Processing

3.9

Is any data transferring outside of the UK?

Choose an item.

Select **yes, no or don't know.** You must determine this so only select don't know if you have further investigations to make but the DPIA will not be approved without this information.

If yes describe where and what additional measures are or will be in place to protect the data.

Click here to enter text.

Personal data may only be transferred outside of the EU in compliance with the conditions for transfer set out in Chapter V of the GDPR. Personal data can be transferred where the organisation receiving the personal data has provided adequate safeguards. Individuals' rights must be enforceable and effective legal remedies for individuals must be available following the transfer. Adequate safeguards may be provided for by:

- ✓ a legally binding agreement between public authorities or bodies;
- ✓ binding corporate rules (agreements governing transfers made between organisations within in a corporate group);
- ✓ standard data protection clauses in the form of template transfer clauses adopted by the Commission;
- ✓ standard data protection clauses in the form of template transfer clauses adopted by a supervisory authority and approved by the Commission;
- ✓ compliance with an approved code of conduct approved by a supervisory authority;
- ✓ certification under an approved certification mechanism as provided for in the GDPR;
- ✓ contractual clauses agreed authorised by the competent supervisory authority; or
- ✓ provisions inserted into administrative arrangements between public authorities or bodies authorised by the competent supervisory authority

DPA

3.10

What Data Processing Agreement is already in place or if none, what agreement will be in place with the organisation and who will be responsible for managing it?

Click here to enter text.

A Processor has obligations as set out by the Data Protection Legislation. A Data Processing Agreement (DPA) is needed whenever a controller uses a processor (a third party who processes personal data on behalf of the controller); there needs to be a written agreement in place. Similarly, if a processor employs another processor it needs to have a written agreement in place. Agreements between controllers and processors ensure that they both understand their obligations, responsibilities and liabilities. They help them to comply with the GDPR, and help controllers to demonstrate their compliance with the GDPR. The use of agreements by controllers and processors may also increase data subjects' confidence in the handling of their personal data.

Agreements must also include a number of terms which have been included in standardised templates available from your IG team or DPO. It is important to remember that every processing activity may be different and whilst there will be common agreements in place each must be assessed to ensure that no changes are needed to the standard template. The Data Processing Schedule is the 'detail' part of the agreement. It is likely that you would only be able to prepare one of these if you had identified all of the required information in a DPIA or obtained it from within the relevant Service Specification.

If a processor fails to meet any of the obligations in the agreement, or acts outside or against the instructions of the controller, then it may be liable to pay damages or compensation in legal proceedings, or be subject to fines

or other penalties or corrective measures. If a processor uses a sub-processor then it will, as the original processor, remain directly liable to the controller for the performance of the sub-processor's obligations.

Privacy Notice

4.1

Describe any changes you plan or need to make to your Privacy Notice and your proposed completion date?

Click here to enter text.

This is an oral or written statement that individuals are given when information about them is collected; it can also be referred to as a "privacy notice" instead. It should as a minimum be a description of how an organisation uses your information. There is a checklist to help you

Fair Processing Notice GDPR-DPA che

Individual Rights

4.2

How will this activity impact on individual rights under the GDPR?

Click here to enter text.

Right of Access

The **right of access**, commonly referred to as subject access, gives individuals the right to obtain a copy of their personal data as well as other supplementary information. It helps individuals to understand how and why you are using their data, and check it is being done lawfully.

What is an individual entitled to?

Individuals have the right to obtain the following:

- confirmation that their personal data is being processed;
- a copy of their personal data; and
- other supplementary information which should be described in a privacy notice

An individual is only entitled to their own personal data, and not to information relating to other people (unless the information is also about them or they are acting on behalf of someone). Therefore, it is important to establish whether the information requested falls within the definition of personal data.

In addition an organisation should provide individuals with the following information:

- the purposes for processing;
- the categories of personal data concerned;
- the recipients or categories of recipient the personal data will be disclosed to;
- the retention period for storing the personal data or, where this is not possible, the criteria for determining how long to store it;
- the existence of their right to request rectification, erasure or restriction or to object to such processing;
- the right to lodge a complaint with the ICO or another supervisory authority;
- information about the source of the data, where it was not obtained directly from the individual;
- the existence of automated decision-making (including profiling); and
- the safeguards provided if transferring personal data to a third country or international organisation

This may already be provided in your privacy notice. For further information go to ICO Guidance.

Data Portability

The **right to data portability** gives individuals the right to receive personal data they have provided to a Controller in a structured, commonly used and machine readable format. It also gives them the right to request

that a Controller transmits this data directly to another Controller.

When does the right apply?
The right to data portability only applies when:

- the lawful basis for processing this information is consent or for the performance of a contract; and
- carrying out the processing by automated means (i.e. excluding paper files)

What does the right apply to?
Information is only within the scope of the right to data portability if it is personal data of the individual that they have provided. Sometimes the personal data an individual has provided will be easy to identify (e.g. their mailing address, username, age). However, the meaning of data 'provided to' is not limited to this. It is also personal data resulting from observation of an individual's activities (e.g. where using a device or service). This may include:

- history of website usage or search activities;
- traffic and location data; or
- 'raw' data processed by connected objects such as smart meters and wearable devices

Does the right apply to anonymous or pseudonymous data?
The right to data portability only applies to personal data. This means that it does not apply to genuinely anonymous data. However, pseudonymous data that can be clearly linked back to an individual (e.g. where that individual provides the respective identifier) is within scope of the right. Further information on this can be found at ICO guidance

Right to Erasure
Individuals have the right to have personal data erased. This is also known as the 'right to be forgotten'. The right is not absolute and only applies in certain circumstances.

When does the right to erasure apply?
Individuals have the right to have their personal data erased if:

- the personal data is no longer necessary for the purpose originally collected or processed for;
- consent was used as the lawful basis for holding the data, and the individual withdraws their consent;
- legitimate interests was used as the lawful basis for processing, the individual objects to the processing of their data, and there is no overriding legitimate interest to continue this processing;
- processing is for direct marketing purposes and the individual objects to that processing;
- processing has been carried out unlawfully;
- it was processed to comply with a legal obligation; or
- to offer information society services to a child

How does the right to erasure apply to data collected from children?
There is an emphasis on the right to have personal data erased if the request relates to data collected from children. This reflects the enhanced protection of children's information, especially in online environments, under the GDPR.

When does the right to erasure not apply?
The right to erasure does not apply if processing is necessary for one of the following reasons:

- to exercise the right of freedom of expression and information;
- to comply with a legal obligation;
- for the performance of a task carried out in the public interest or in the exercise of official authority;
- for archiving purposes in the public interest, scientific research historical research or statistical purposes where erasure is likely to render impossible or seriously impair the achievement of that processing; or
- for the establishment, exercise or defence of legal claims

The GDPR also specifies two circumstances where the right to erasure will not apply to special category data:

- if the processing is necessary for public health purposes in the public interest (e.g. protecting against

serious cross-border threats to health, or ensuring high standards of quality and safety of health care and of medicinal products or medical devices); or

- if the processing is necessary for the purposes of preventative or occupational medicine (e.g. where the processing is necessary for the working capacity of an employee; for medical diagnosis; for the provision of health or social care; or for the management of health or social care systems or services). This only applies where the data is being processed by or under the responsibility of a professional subject to a legal obligation of professional secrecy (e.g. a health professional)

If Article 6 1 (e) and Article 9 2 (h) are being used in 1.2 and 1.11 above then it is likely that the right to erasure will not apply to this data. Further information can be found at ICO guidance

Right to restrict processing

Individuals have the right to request the restriction of the processing of their personal data in the following circumstances:

- they contest the accuracy of their personal data and this needs verifying;
- the data has been unlawfully processed and the individual opposes erasure and requests restriction instead;
- the personal data is no longer needed but the individual needs it kept it in order to establish, exercise or defend a legal claim; or
- they have objected to the processing of their data and an organisation is considering whether their legitimate grounds override those of the individual

Further information on this can be found at ICO guidance.

What is automated individual decision-making and profiling?

Automated individual decision-making is a decision made by automated means without any human involvement. Examples of this include:

- an online decision to award a loan; and
- a recruitment aptitude test which uses pre-programmed algorithms and criteria

Automated individual decision-making does not have to involve profiling, although it often will do.

The GDPR says that profiling is "Any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements."

ICO guidance on automated decisions and profiling

As well as restricting the circumstances in which you can carry out solely automated individual decision-making the GDPR also:

- requires you to give individuals specific information about the processing;
- obliges you to take steps to prevent errors, bias and discrimination; and
- gives individuals rights to challenge and request a review of the decision

These provisions are designed to increase individuals' understanding of how you might be using their personal data.

You must:

- provide meaningful information about the logic involved in the decision-making process, as well as the significance and the envisaged consequences for the individual;
- use appropriate mathematical or statistical procedures;

In addition you must ensure that individuals can:

- obtain human intervention;
- express their point of view; and

- obtain an explanation of the decision and challenge it;

Records Management

4.3
How long is the data/information to be retained?

Click here to enter text.
You must be able to identify how long any records created as part of this activity need to be kept. There is a records management code of practice that will help you determine what type of record is being created and how long it should be kept Records Management Code of Practice

4.4
How will the data/information be archived?

Click here to enter text.
Depending on the type of record or information involved in your proposed activity, there may be a requirement for it to be archived either permanently or temporarily as part of, or at the end of the retention period. The records management code of practice may include information to support you with this. The National Archives have also produced guidance that may help you The National Archives

4.5
What is the process for the destruction of records?

Click here to enter text.
Are there are any agreements in place with existing suppliers of record or data destructions services. This may include licensed shredding companies or those who provide confidential waste services. This will only be sufficient for paper records and consideration must be given to the requirements necessary for electronically held information. Your IT provider/software provider/third party Processor must have appropriate measures in place to ensure that any electronic information is deleted appropriately and not saved in a server storage facility. NHS Digital have issued guidance for organisations on what they should consider Destruction Guidance

4.6
What will happen to the data/information if any part of your activity ends?

Click here to enter text.
It is vital to consider what would happen should the organisation or the service cease to operate. This is particularly important if the activity involves a short term piece of work, a proof of concept or a pilot. The Controller must ensure that any record/information/data created as part of the activity is safeguarded and saved for the correct amount of time, especially if patient information is involved and there are set retention and archiving periods. An organisation should consider this very early in the setting up of the service. They are responsible if they are considered to be Controllers. If there is a Processor involved then it should be stipulated in the Data Processing Agreement what arrangements will be in place to preserve and safeguard any activity related data/information.

Direct Marketing

4.7
Will you use any data for direct marketing purposes?

Choose an item.
Select **yes, no or don't know.** You must determine this so only select don't know if you have further investigations to make but the DPIA will not be approved without this information.

If yes please detail.

Click here to enter text.
Add detail of any proposed marketing. You can find out about what constitutes direct marketing by reading the

ICO guidance in direct marketing.

Risks and issues

5.1

What risks and issues have you identified?

The DPO can provide advice to help complete this section and the SIRO should approve any measures to mitigate potential risks. You can replace the matrix and use your own risk management assessment process to determine the level of risk that may be caused by all or some of the activities described in the DPIA.

When identifying data security and protection and cyber risks, consideration should be given to the National Cyber Security Centre's (NCSC) guidance on information risk management (https://www.ncsc.gov.uk/collection/risk-management/a-basic-risk-assessment-and-management-method).

An example is included here to help you consider the risks.

Example 3x3 risk matrix				
Likelihood of harm	Probable	Medium	High	High
	Possible	Low	Medium	High
	Remote	Low	Low	Medium
		Minimal	Significant	Severe
		Severity of harm		

Describe the source of risk and nature of potential impact on individuals. EXAMPLES Click here to enter text.	Likelihood of harm Choose an item. Remote Possible Probable	Severity of harm Choose an item. Minimal Significant Severe	Overall risk Choose an item. Low Medium High
Patient information may be shared without their knowledge.	Possible	Significant	Medium
The Practice uses a Processor that is not IG compliant and does not use secure recording methods.	Possible	Severe	High

5.2

Identify additional measures you could take to reduce or eliminate risks identified as amber or above in 5.1				
Risk Click here to enter text.	**Options to reduce or eliminate risk** Click here to enter text.	**Effect on risk** Choose an item. Eliminated Reduced Accepted	**Residual risk** Choose an item. Low Medium High	**Measure approved (SIRO)** Choose an item. Yes No Needs escalating Needs more consideration
Patient information may be shared without their knowledge.	1. Consider if Patient Consent is appropriate 2. Update my Fair Processing Notice 3. Produce a Patient leaflet	Reduced	Low	Yes
The Practice uses a	1. Ask Supplier for details of	Reduced	Low	Yes

Processor that is not IG compliant and does not use secure recording methods.	their security arrangements 2. Check if the Supplier has done a DSP toolkit 3. Make sure there is a contract and a Data Processing Agreement with IG clauses in it 4. Ask the Supplier to complete some parts of the DPIA, particularly section 3.			

5.3
What if anything would affect this piece of work?

Click here to enter text.
Describe anything that you feel can support this DPIA now or may alter its approach in the future.

5.4
Do you have any further comments to make that do not fit elsewhere in the DPIA? (ie onboarding/offboarding and compliance management, cyber incident response and recovery testing in relation to the supply chain)

Click here to enter text.

Consultation

6.1
Have you consulted with any external organisation about this DPIA?

Choose an item.
Select **yes, no or don't know.**

If yes, who and what was the outcome? If no or don't know, detail why consultation was not felt necessary.

Click here to enter text.
The Controller must "seek the views of data subjects or their representatives where appropriate". Those views could be sought through a variety of means, depending on the context (e.g. a generic study or questionnaire, a question to the Patient forum, or a survey sent to your Patients or left in reception) ensuring that the Controller has a lawful basis for processing any personal data involved in seeking such views. If the Controller's final decision differs from the views of the data subjects, its reasons for going ahead or not should be documented; - the Controller should also document its justification for not seeking the views of data subjects, if it decides that this is not appropriate, for example if doing so would compromise the confidentiality of companies' business plans, or would be disproportionate or impracticable. Further information can be found at the links of the ICO Guidance

6.2
Will you need to discuss the DPIA or the processing with the Information Commissioners Office?

Choose an item.
Select **yes, no or don't know.**

If yes, explain why you have come to this conclusion.
Click here to enter text.

If when you do your risk assessment, you find that a high risk has been identified that you cannot mitigate for, you must consult with the DPO first if you feel this needs to be discussed with the ICO. Further information can be found in the ICO Guidance

Data Protection Officer Comments and observations

7.1 **Comments/observations/specific issues**	Click here to enter text. This will be used by the DPO to highlight further matters to be discussed.

Outcome

Based on the information contained in this DPIA along with any supporting documents, you have determined that the outcome is as follows:

Choose an item.
A) There are no further actions needed and we can proceed
B) There are further actions that need to be taken but we can proceed
C) We should not proceed at present
D) We cannot determine an outcome at present

If you have selected item B), C) or D) then please add comments as to why you made that selection

Click here to enter text.

We believe there are

Choose an item.
A) No unmitigated or identified risks outstanding
B) Risks that need further consideration and management
C) Considerable risks that need further consultation with the ICO

If you have selected item B) or C) then list these in the amber boxes below and then consider additional measures you could take and include these in the green boxes below

Residual risks and nature of potential impact on individuals (b and c). Include associated compliance and corporate risks as necessary.	**Likelihood of harm** Remote Possible Probable	**Severity of harm** Minimal Significant Severe	**Overall risk** Low Medium High
Click here to enter text.	Choose an item.	Choose an item.	Choose an item.
Click here to enter text.	Choose an item.	Choose an item.	Choose an item.

Additional measures you could take to reduce or eliminate residual risks identified as medium or high risk above (b and c)

Risk (from box above)	**Options to reduce or eliminate risk**	**Effect on risk** Eliminated Reduced Accepted	**Residual risk** Low Medium High	**Measure approved (SIRO)** Yes No Needs escalating Needs more consideration
Click here to enter text.	Click here to enter text.	Choose an item.	Choose an item.	
Click here to enter text.	Click here to enter text.	Choose an item.	Choose an item.	

Signed and approved on behalf of: (add organisation name) Click here to enter text.

Name: (add name of signatory) Click here to enter text.

Job Title: (the signatory should be someone designated to take decisions of this nature on behalf of the

organisation) Click here to enter text.

Signature: Click here to enter text. Date: Click here to enter a date.

Please note:

You should ensure that the Information Asset Register and Data Flow Mapping Schedules for your service area are updated where this is relevant. Talk to your Information Asset Owner.

This DPIA can be disclosed if requested under the Freedom of Information Act (2000). If there are any exemptions that should be considered to prevent disclosure detail them here:
Click here to enter text.

End of Guidance

Document Control

This document was created by NHS South Central and West Commissioning Support Unit (SCW) and as such the IP rights of this document belong to SCW.

Document Name	Version	Status	Author
DPIA Template Guidance	6.0	Published	NHS SCW Information Governance Services
Document objectives:	This document supports staff in compliance with Data Protection legislation, achieving best practice in the area of Information Governance and in meeting the requirements of the Data Security and Protection Toolkit		
Target audience:	All staff		
Monitoring arrangements and indicators:	This document will be monitored by NHS SCW Information Governance Services to ensure any legislative changes that occur before the review date are incorporated.		
Approved by:	IGSG	Date: [26/07/2023]	
Ratified by:	Audit and Risk Committee	Date:	
Date issued:	[xx/xx/2023]		
Review date:	July 2025		

Change record

Date	Author	Version	Page	Reason for Change
07/10/2020	IG team	6	Various	Added SCW branding and colour scheme; amended section heading for 1.4 to add 'Processor'; added '(please specify)' for reasonable expectations if selected under section 1.7; added 500+ and 1000+ options to section 1.10; removed reference to organisations listed only in section 3.1 from sections 3.2, 3.3 and 3.4 to reflect the need to include information on all organisations involved and not just Processors; removal of reference to SKYPE in section 2.7; added document control to page 35.
26/07/2023	DPO	6.1	5	Amended to include completing a DPIA early in the project and requirement for the author to be a member of staff with enough authority over a project to effect change.