

## STANDARD OPERATING PROCEDURE DATA PROTECTION IMPACT ASSESSMENTS

<b>Document Reference</b>	SOP16-005
<b>Version Number</b>	1.7
<b>Author/Lead Job Title</b>	Tracey O'Mullane Information Governance Officer
<b>Instigated by: Date Instigated:</b>	Information Governance Committee December 2015
<b>Date Last Reviewed:</b>	15 May 2024
<b>Date of Next Review:</b>	May 2027
<b>Consultation:</b>	IG Group
<b>Ratified and Quality Checked by: Date Ratified:</b>	Information Governance Group 15 May 2024
<b>Name of Trust Strategy / Policy / Guidelines this SOP refers to:</b>	

**VALIDITY – All local SOPS should be accessed via the Trust intranet**

### CHANGE RECORD

Version	Date	Change details
1.1	March 2017	Annual review. No changes required.
1.2	February 2018	Annual review. Minor changes. Procedure into new format. Update the title of the IG Committee to IG Group.
1.3	September 2018	Updated in line with requirements set out in the Data Security and Protection Toolkit. DPIA template updated to incorporate GDPR/DPA 2018
1.4	November 2019	Added into the introduction the accountability principle under GDPR. Expanded the screening questions to provide further information and extra instances of when a DPIA would be required. Added online identifiers under question 3. Added in Article 6 and 9 under questions 15. Added further questions in relation to the location of the data (qu29) and in relation to any training/instruction on the system (qu35). Added in a risk assessment to document any risks identified in the DPIA.
1.5	November 2020	Annual review. Example risks added as an appendix.
1.6	July 2022	Added cyber fraud risk and transactional monitoring question under Section A. Updated GDPR to UK GDPR. Added third party processor's name at question 7. Added Other lawful basis option to question 15. Updated reference at question 38. Added cyber fraud definition to Appendix C. Approved at Information Governance Group (July 2022).
1.7	May 2024	Expanded the Introduction to include examples of when a DPIA would be required. Added question to identify the type of change to Section A. Added penetration testing question (qu 33) Added business continuity/disaster recovery testing question (qu42). Approved at Information Governance Group (15 May 2024).

## Contents

1. INTRODUCTION.....	3
2. PURPOSE .....	3
3. PROCEDURE .....	4
4. REFERENCES/EVIDENCE/GLOSSARY/DEFINITIONS.....	4
5. RELEVANT HFT POLICIES/PROCEDURES/PROTOCOLS/GUIDELINES.....	4
Appendix A – Data Protection Impact Assessment (DPIA) Screening Questions .....	5
Appendix B – Data Protection Impact Assessment .....	6
Appendix C – Example Risks .....	17

## 1. INTRODUCTION

All organisations experience change in one form or another. Rapidly changing technology has a major impact on processes and systems already in place, often requiring change simply to keep up to date and to enable the safe and secure processing of personal data.

Systems and processes that involve using personal or special category information or captures biometric information that can be used to identify an individual such as an image, voice; or that introduce new technologies e.g. artificial intelligence; or a new App create privacy issues and concerns from individuals, to provide reassurance it is essential the minimum personal data is processed, and that processing is transparent, allowing individuals to monitor what is being done with their data.

It is vitally important that all proposed changes to Trust processes and/or information assets are assessed to ensure that confidentiality, integrity and accessibility of information is maintained. This will be done by undertaking a Data Protection Impact Assessment (DPIA) prior to the introduction of new processes, software or hardware.

UK [General Data Protection Regulation \(UK GDPR\)](#) also requires organisation to complete a DPIA before carrying out types of processing that is likely to result in high risk to individual's interests.

Under UK GDPR, the Trust must be able to demonstrate compliance with the principles (accountability). One of the ways the Trust does this is by carrying out a DPIA for any changes in the use of personal data.

This process is a mandated requirement on the Data Security and Protection Toolkit to ensure that privacy concerns have been considered and actioned to ensure the security and confidentiality of the personal identifiable information.

A DPIA integrates data protection by design and by default from the outset rather than an expensive bolt on at the end.

A DPIA will ensure that: -

- the impact on an individual's privacy is assessed and minimised with the minimum necessary personal data and pseudonymisation where possible.
- personal information is protected from unlawful or unauthorised access and from accidental loss, destruction or damage
- personal information can be located and retrieved in a timely manner
- personal information held is relevant, accurate and valid
- personal information is disposed of through archiving or destruction when it is no longer required

## 2. PURPOSE

This procedure documents the actions to be taken before introducing new processes, software or hardware that involve personal data to ensure data protection by design and by default.

### **3. PROCEDURE**

The Data Protection Impact Assessment in Appendix B must be completed for any new or change in service which plans to utilise personal confidential information. It must be completed as soon as the new service or change is identified by the Project Manager, System Manager or Information Asset Owner. The screening questions in Appendix A will help to determine whether a DPIA is required.

Please complete all questions with as much detail as possible and return the completed form to: [hnf-tr.IGTeam@nhs.net](mailto:hnf-tr.IGTeam@nhs.net)

The Information Governance Team will review the DPIA and request any further information.

Data Protection Impact Assessments will be agreed by the Information Governance Group or Senior Information Risk Owner.

Information Governance will submit all completed Data Protection Impact Assessments to the Communications Team for publication on the Trust's website. Commercial sensitive information such as security measures or intended product development should be redacted.

### **4. REFERENCES/EVIDENCE/GLOSSARY/DEFINITIONS**

Data Security and Protection Toolkit – Standard 1.3  
Data Protection Act 2018  
UK General Data Protection Regulation

Glossary – see Appendix B

### **5. RELEVANT HFT POLICIES/PROCEDURES/PROTOCOLS/GUIDELINES**

Caldicott and Data Protection Policy  
Safe Haven Procedure  
Information Security and Risk Policy

## Appendix A – Data Protection Impact Assessment (DPIA) Screening Questions

The below screening questions should be used to inform whether a DPIA is necessary. This is not an exhaustive list therefore in the event of uncertainty, completion of a DPIA is recommended.

<b>Title</b>	Click here to enter text.
<b>Brief description</b>	Click here to enter text.

### Screening completed by

<b>Name</b>	Click here to enter text.
<b>Title</b>	Click here to enter text.
<b>Department</b>	Click here to enter text.
<b>Email</b>	Click here to enter text.
<b>Review date</b>	Click here to enter text.

Marking any of these questions is an indication that a DPIA is required:

Screening Questions		Tick
1	Will the project involve the collection of new identifiable or potentially identifiable information about individuals?	<input type="checkbox"/>
2	Will the project compel individuals to provide information about themselves or involve the processing of personal data not obtained directly from the individual? i.e. where they will have little awareness or choice or it is impossible or would involve disproportionate effort to inform the individuals that the processing is taking place.	<input type="checkbox"/>
3	Will identifiable information about individuals be shared with other organisations or people who have not previously had routine access to the information?	<input type="checkbox"/>
4	Are you using information about individuals for a purpose it is not currently used for or in a new way? i.e. using data collected to provide care for an evaluation of service development; data matching from multiple sources.	<input type="checkbox"/>
5	Where information about individuals is being used, would this be likely to raise privacy concerns or expectations? i.e. will it include health records, criminal records or other information that people may consider to be sensitive and private and may cause them concern or distress.	<input type="checkbox"/>
6	Will the project require you to contact individuals in ways which they may find intrusive? i.e. telephoning or emailing them without their prior consent.	<input type="checkbox"/>
7	Will the project result in you making decisions in ways which can have a significant impact on individuals? i.e. will it affect the care a person receives.	<input type="checkbox"/>
8	Does the project involve you using new technology which might be perceived as being privacy intrusive? i.e. using biometrics, facial recognition, artificial intelligence or automated decision making.	<input type="checkbox"/>
9.	Is a service being transferred to a new supplier (re-contracted) and the end of an existing contract or the processing of identifiable/potentially identifiable data being moved to a new organisation (but with same staff and processes)	<input type="checkbox"/>
10.	Will the project involve systematic monitoring of a publicly accessible area on a large scale? i.e. use of CCTV.	<input type="checkbox"/>
11.	Will the project involve the targeting of children or other vulnerable individuals i.e. for marketing purposes, profiling or other automated decision making?	<input type="checkbox"/>

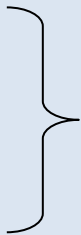
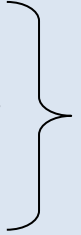
***Please retain a copy of this questionnaire within your project/system documentation.***

## Appendix B – Data Protection Impact Assessment

### Section A - New/Change of System/Project General Details

<b>Name of system/project/process:</b>			
<b>Is the system/project a:</b>	<input type="checkbox"/> System	<input type="checkbox"/> App	<input type="checkbox"/> New technology <input type="checkbox"/> Process
<b>Objective:</b>			
<b>Background:</b> <small>Why is the new system / change in system required? Is there an approved business case?</small>			
<b>Benefits:</b>			
<b>Constraints:</b>			
<b>Relationships:</b> <small>(for example, with other Trust's, organisations)</small>			
<b>Quality expectations:</b>			
<b>Cyber Fraud Risk:</b> <b>Is the system likely to be susceptible to cyber criminals?</b> <small>(for example fraud risk of financial gain)</small>	Yes <input type="checkbox"/> No <input type="checkbox"/>	If yes, does the system include transactional monitoring?	Yes <input type="checkbox"/> No <input type="checkbox"/>
<b>Expected "go-live" date.</b>			
<b>Cross reference to other projects:</b>			
<b>Project Manager:</b>	Name:		
	Title:		
	Department:		
	Telephone:		
	Email		
<b>Information Asset Owner:</b> <small>(All systems/assets must have an Information Asset Owner (IAO).</small>	Name:		
	Title:		
	Department:		
	Telephone:		
	Email		
<b>Information Asset Administrator:</b> <small>(It is necessary that there is a deputy in place for when the IAO is absent from the workplace for whatever reason)</small>	Name:		
	Title:		
	Department:		
	Telephone:		
	Email		
<b>Customers and stakeholders:</b>			

## Section B - Data Protection Impact Assessment Key Questions

Question	Response
<b>Data Items</b>	
<p><b>1. Will the system/project/process (will now be referred to thereafter as 'asset') contain Personal Confidential Data or Sensitive Data?</b></p> <p style="color: blue;">If answered 'No' you do not need to complete any further information as DPIA is not required.</p>	<p><input type="checkbox"/> Yes <span style="margin-left: 200px;"><input type="checkbox"/> No</span></p> <p>If yes, who will this data relate to:</p> <p><input type="checkbox"/> Patient</p> <p><input type="checkbox"/> Staff</p> <p><input type="checkbox"/> Other (specify)</p>
<p><b>2. Please state purpose for the collection of the data:</b></p> <p style="color: blue;">for example, patient treatment, health administration, research, audit, staff administration</p>	
<p><b>3. Please tick the data items that are held in the system</b></p> <div style="display: flex; justify-content: space-between; align-items: center; margin-top: 20px;"> <div style="text-align: center;"> <p><b>Personal</b></p>  </div> <div style="width: 80%;"> <p><input type="checkbox"/> Name <span style="margin-left: 100px;"><input type="checkbox"/> Address</span></p> <p><input type="checkbox"/> Post Code <span style="margin-left: 100px;"><input type="checkbox"/> Date of Birth</span></p> <p><input type="checkbox"/> GP <span style="margin-left: 100px;"><input type="checkbox"/> Consultant</span></p> <p><input type="checkbox"/> Next of Kin <span style="margin-left: 100px;"><input type="checkbox"/> Hospital (District) No.</span></p> <p><input type="checkbox"/> Sex <span style="margin-left: 100px;"><input type="checkbox"/> NHS Number</span></p> <p><input type="checkbox"/> National Insurance No. <span style="margin-left: 100px;"><input type="checkbox"/> Online identifier (e.g. IP address)</span></p> </div> </div> <div style="display: flex; justify-content: space-between; align-items: center; margin-top: 20px;"> <div style="text-align: center;"> <p><b>Special Category</b></p>  </div> <div style="width: 80%;"> <p><input type="checkbox"/> Health data <span style="margin-left: 100px;"><input type="checkbox"/> Sex life and sexual orientation</span></p> <p><input type="checkbox"/> Political opinions <span style="margin-left: 100px;"><input type="checkbox"/> Religion</span></p> <p><input type="checkbox"/> Biometric data <span style="margin-left: 100px;"><input type="checkbox"/> Racial or ethnic Origin</span></p> <p><input type="checkbox"/> Genetic data <span style="margin-left: 100px;"><input type="checkbox"/> Trade Union membership</span></p> </div> </div> <p style="margin-top: 20px;">Other (please state here):</p>	
<p><b>4. Will the asset collect new personal data items which have not been collected before?</b></p>	<p><input type="checkbox"/> Yes <span style="margin-left: 200px;"><input type="checkbox"/> No</span></p> <p>If yes, please give details:</p>
<p><b>5. What checks have been made regarding the adequacy,</b></p>	

relevance and necessity for the collection of personal and/or sensitive data for this asset?	
6. How will the information be kept up to date and checked for accuracy and completeness?	
<b>Data processing</b>	
7. Will a third party be processing the data?	<input type="checkbox"/> Yes <input type="checkbox"/> No Name of third party:
8. Is the third party contract/supplier of the system on the Register of Fee Payers with the Information Commissioner? What is their registration number?	<input type="checkbox"/> Yes <input type="checkbox"/> No Data Protection Act Registration Number:
9. Has the third party supplier completed a Data Security and Protection Toolkit?	<input type="checkbox"/> Yes <input type="checkbox"/> No If yes, please give assessment status:
10. Does the third party/supplier contracts contain all the necessary Information Governance clauses including information about Data Protection and Freedom of Information?	<input type="checkbox"/> Yes <input type="checkbox"/> No Is the contract based on or utilise the NHS Standard Contract? <input type="checkbox"/> Yes <input type="checkbox"/> No
11. Will other third parties (not already identified) have access to the data? (include any external organisations)	<input type="checkbox"/> Yes <input type="checkbox"/> No If so, for what purpose? Please list organisations and by what means of transfer
12. Who provides the information for the asset?	<input type="checkbox"/> Patient <input type="checkbox"/> Staff <input type="checkbox"/> Others – Please specify e.g. <a href="#">Interfaces from PAS</a>
<b>Confidentiality</b>	
13. Please outline how individuals will be informed and kept informed about how their data will be processed. (A copy of the privacy notice/leaflet must be provided)	



<p><b>14. Does the asset involve new or changed data collection policies that may be unclear or intrusive?</b></p> <p>Are all data items clearly defined?</p> <p>Is there a wide range of special category data being included?</p>	<p><input type="checkbox"/> Yes <input type="checkbox"/> No</p>
<p><b>15. Are you relying on individuals (patients/staff) to provide consent for the processing of personal identifiable or sensitive data?</b></p>	<p><input type="checkbox"/> Yes <input type="checkbox"/> No</p> <p>Where consent <i>is</i> being sought:</p> <p>Is the consent explicit? <input type="checkbox"/> Yes <input type="checkbox"/> No</p> <p>Where explicit consent is <i>not</i> being sought:</p> <p>a. Will identifiable data only be handled within the patient's direct care team (in accordance with the Common law duty of confidence)</p> <p><input type="checkbox"/> Yes <input type="checkbox"/> No</p> <p>b. Which legal basis/justification is in place to permit this processing (in accordance with Data Protection Act/General Data Protection Regulation)?</p> <p>Article 6</p> <p><input type="checkbox"/> Performance of contract</p> <p><input type="checkbox"/> Legal obligation</p> <p><input type="checkbox"/> Vital interests</p> <p><input type="checkbox"/> Public task</p> <p><input type="checkbox"/> Legitimate interests (Public bodies cannot rely on this basis for the performance of their tasks as a public authority)</p> <p>Article 9 if special category of data is processed.</p> <p><input type="checkbox"/> Employment, social security and social protection law</p> <p><input type="checkbox"/> Vital interests</p> <p><input type="checkbox"/> Non for profit body</p> <p><input type="checkbox"/> Data made public by the data subject</p> <p><input type="checkbox"/> Exercise/defend legal claims</p> <p><input type="checkbox"/> Substantial public interest</p> <p><input type="checkbox"/> Provision of health or social care</p> <p><input type="checkbox"/> Public health</p> <p><input type="checkbox"/> Archiving/research/statistical</p> <p><input type="checkbox"/> Other lawful basis</p> <p>State lawful basis:</p>
<p><b>16. If yes, how will that consent be obtained? Please state:</b></p> <p>Please include a copy of any consent forms</p>	

<p><b>17. Will the consent cover all the proposed processing and sharing/disclosures</b></p>	<p><input type="checkbox"/> Yes <input type="checkbox"/> No</p>
<p><b>18. How will consent and non-consent be recorded and respected?</b></p>	
<p><b>19. What arrangements are in place to process subject access requests?</b></p>	
<p><b>20. Is automated decision making used?</b></p> <p><b>If yes, how do you notify the individual?</b></p> <p><b>Please also outline what arrangements are available to the enable the individual access and to extract data (in a standard file format)</b></p> <p><b>Please detail any profiling that may take place through automated processing.</b></p>	<p><input type="checkbox"/> Yes <input type="checkbox"/> No</p>
<p><b>21. What procedures are in place for the rectifying/blocking of data by individual request or court order?</b></p>	
<p><b>Engagement</b></p>	
<p><b>22. Has stakeholder engagement taken place?</b></p>	<p><input type="checkbox"/> Yes <input type="checkbox"/> No</p> <p>If yes, how have any issues identified by stakeholders been considered?</p> <p>If no, please outline any plans in the near future to seek stakeholder feedback.</p>
<p><b>Data Sharing</b></p>	
<p><b>23. Does the project involve any new information sharing between stakeholder organisations?</b></p>	<p><input type="checkbox"/> Yes <input type="checkbox"/> No</p> <p>If yes, please describe:</p> <p>Please provide a data flow diagram showing how identifiable information would flow.</p>

## Data Linkage

**24. Does the asset involve new linkage of personal data with data in other collections, or is there significant changes in data linkages?**

The degree of concern is higher where data is transferred out of its original context (e.g. the sharing and merging of datasets can allow for a much wider set of information than needed and identifiers might be collected/linked which prevents personal data being kept anonymously).

Yes

No

If yes, please provide a data flow diagram showing how identifiable information would flow.

## Information Security

**25. Who will have access to the data within the system/project?**  
Please refer to roles/job titles.

**26. How will access to the system be provided?**

**Does the system support MFA?**  
If so, please provide details (type of MFA, which accounts will it be applied to)

**How will starters/leavers be managed?**

**27. Is there a useable audit trail in place for the asset.** For example, to identify who has accessed a record?

Yes

No

**28. Where will the information be kept/stored/accessed?**

On paper

On a database saved on a network folder/drive

Website

On a dedicated system saved to the network

Other – please state below:

**29. Where is this information located? Please detail the countries where the servers are located.**

<p><b>30. Please state by which method the information will be transported</b></p>	<p> <input type="checkbox"/> Fax                    <input type="checkbox"/> Email  <input type="checkbox"/> Via NHS Mail  <input type="checkbox"/> Website                    <input type="checkbox"/> Via courier  <input type="checkbox"/> By hand                    <input type="checkbox"/> Via post – internal  <input type="checkbox"/> Via telephone                    <input type="checkbox"/> Via post - external  <input type="checkbox"/> Other – please state below:       </p>
<p><b>31. Does the asset involve new privacy-enhancing technologies?</b></p> <p>Encryption; 2 factor authentication, pseudonymisation</p>	<p> <input type="checkbox"/> Yes                    <input type="checkbox"/> No          If yes, please give details:       </p>
<p><b>32. Is there a documented System Level Security Policy (SLSP) or process for this project? A SLSP is required for new systems</b></p>	<p> <input type="checkbox"/> Yes                    <input type="checkbox"/> No  <input type="checkbox"/> Not applicable          If yes, please provide a copy.       </p>
<p><b>33. Is annual Penetration Testing undertaken?</b></p>	<p> <input type="checkbox"/> Yes                    <input type="checkbox"/> No                    <input type="checkbox"/> N/A          Date of last test:       </p>
<p><b>34. Is there a Security Management Policy and Access Policy in place? Please state policy titles.</b></p>	<p> <input type="checkbox"/> Yes                    <input type="checkbox"/> No       </p>
<p><b>35. Are there procedures in place to recover data (both electronic /paper) which may be damaged through:</b></p> <ul style="list-style-type: none"> <li>• Human error</li> <li>• Computer virus</li> <li>• Network failure</li> <li>• Theft</li> <li>• Fire</li> <li>• Flood</li> <li>• Other disaster</li> </ul> <p>Please provide policy titles.</p>	<p> <input type="checkbox"/> Yes                    <input type="checkbox"/> No       </p>
<p><b>36. What training and instructions are necessary to ensure that staff know how to operate a new system securely?</b></p>	

## Privacy and Electronic Communications Regulations

**37. Do you intend to send direct marketing messages by electronic means? This includes both live and pre-recorded telephone calls, fax, email, text message and picture (including video)?**

Yes  No  
 If yes, what communications will be sent?  
  
 Will consent be sought prior to this?  
 Yes  No  
 If no, please explain why consent is not being sought first:

**38. Does the asset comply with privacy laws such as the Privacy and Electronic Communications Regulations 2003 (see appendix for definition)**

Yes  No

## Records Management

**39. What are the retention periods (what is the minimum timescale) for this data? (please refer to the Records Management Code of Practice 2021) and list the retention period for the identifiable project datasets**

**40. How will the data be destroyed when it is no longer required?**

## Business Continuity

**41. Is there a contingency plan / backup policy, or business continuity plan in place to manage the effect of an unforeseen event? Please provide a copy.**

Yes  No

**42. Is annual testing of the business continuity/disaster recovery plan undertaken?**

Yes  No  N/A  
 Date of last test:

## Open Data

**43. Will identifiable/potentially identifiable data from the project/system be released as Open Data (placed in to the public domain)?**

Yes  No

## Data Processing Outside of the EEA

44. Are you transferring any personal and / or sensitive data to a country outside the European Economic Area (EEA)?

Yes  No  
If yes, where?

45. What is the data to be transferred to the non EEA country?

46. Are measures in place to mitigate risks and ensure an adequate level of security when the data is transferred to this country?

Yes  No  
 Not applicable

## NHS Number Verification Status

Organisations should risk assess their own and new systems and processes, and implement appropriate solutions. It is recommendation to ensure all NHS Numbers are verified to support safer patient identification practices.

If the answer to any of the below questions is Yes then the system is an applicable system and the NHS Number standard applies

47. Does the system act as a master index to send patient identifiable data and NHS Numbers to other systems?

48. Will the system be used to produce hard-copy outputs containing patient identifiable data (this includes patient facing information such as appointment letters)

49. Does the system need to transfer information between organisations

50. Will the NHS Number ever be required to be stored against patient identifiable data in the system (e.g. for audit purposes)

## Clinical Safety

The organisation must be compliant with the mandated information standards (DCB 0129 and DCB 0160). Appropriate mechanisms should be in place to ensure patient safety during the whole life cycle of a Healthcare IT system which is led by a suitably qualified experienced clinician. The standards are to be followed for all implementations, updates, upgrades, and decommissioning of systems. The standards apply to any Healthcare IT system developed, deployed or used in the trust including those not implemented by IT programmes.

51. Is the implementation a First of Type or Early Adopter	
52. Has the supplier safety documentation been reviewed	
53. Does the implementation have a Clinical Risk Management Plan?	
54. How will compliance with Data Set Change Notice (DSCN) 18/2009 Patient Safety Risk Management System – Deployment and Use of Health Software be managed.	
<b>DIGITAL DELIVERY GROUP</b>	
55. Has the project been approved by the Digital Delivery Group	<input type="checkbox"/> Yes <input type="checkbox"/> No If No, please detail why this isn't required.

<b>Risk Assessment: Detail any risks identified in the DPIA process? See Appendix C for example risks</b>			
Risk	Measures to reduce/eliminate the risk	Result: Is the risk eliminated, reduced or accepted	Measure approved: Yes/No

**Evaluation**

<b>56. Is the DPIA approved?</b>  If not, please state the reasons why and the action plan put in place to ensure the DPIA can be approved	<input type="checkbox"/> Yes <input type="checkbox"/> No
--	--

**Form completed by:**

Name	
Title	
Signature	
Date	

**Information Governance Team Review**

Name	
Title	
Signature	
Date	

**Information Governance Group Approval**

Date of IG Group approval	
Any data to be redacted	
Date of publication	



## Appendix C – Example Risks

### Types of Privacy risks

- Risks affecting individuals or other third parties, for example; misuse or overuse of their personal data, loss of anonymity, intrusion into private life through monitoring activities, lack of transparency.
- Compliance risks e.g. breach of the GDPR
- Corporate risks (to the organisation), for example; failure of the project and associated costs, legal penalties or claims, damage to reputation, loss of trust of patients or the public.

### Risk to individuals

- Inadequate disclosure controls increase the likelihood of information being shared inappropriately.
- The context in which information is used or disclosed can change over time, leading to it being used for different purposes without people's knowledge.
- New surveillance methods may be an unjustified intrusion on their privacy.
- Measures taken against individuals as a result of collecting information about them might be seen as intrusive.
- The sharing and merging of datasets can allow organisations to collect a much wider set of information than individuals might expect.
- Identifiers might be collected and linked which prevent people from using a service anonymously.
- Vulnerable people may be particularly concerned about the risks of identification or the disclosure of information.
- Collecting information and linking identifiers might mean that an organisation is no longer using information which is safely anonymised.
- Information which is collected and stored unnecessarily, or is not properly managed so that duplicate records are created, presents a greater security risk.
- If a retention period is not established information might be used for longer than necessary.

### Corporate risks

- Non-compliance with the data protection legislation can lead to sanctions, fines and reputational damage.
- Problems which are only identified after the project has launched are more likely to require expensive fixes.
- The use of biometric information or potentially intrusive tracking technologies may cause increased concern and cause people to avoid engaging with the organisation.
- Information which is collected and stored unnecessarily, or is not properly managed so that duplicate records are created, is less useful to the business.
- Public distrust about how information is used can damage an organisation's reputation and lead to loss of business.
- Data losses which damage individuals could lead to claims for compensation.

### Compliance risks

- Non-compliance with the Data Protection Act 2018/UK General Data Protection Regulation (EU) 2016/679.
- Non-compliance with the Common Law Duty of Confidentiality.
- Non-compliance with the Privacy and Electronic Communications Regulations (PECR).
- Non-compliance with sector specific legislation or standards.
- Non-compliance with Human Rights Act 1998 and Equality Act 2010.

## Appendix C – Glossary

Item	Definition
Anonymity	Information may be used more freely if the subject of the information is not identifiable in any way – this is anonymised data. However, even where such obvious identifiers are missing, rare diseases, drug treatments or statistical analyses which may have very small numbers within a small population may allow individuals to be identified. A combination of items increases the chances of patient identification. When anonymised data will serve the purpose, health professionals must anonymise data and whilst it is not necessary to seek consent, general information about when anonymised data will be used should be made available to patients.
Authentication Requirements	An identifier enables organisations to collate data about an individual. There are increasingly onerous registration processes and document production requirements imposed to ensure the correct person can have, for example, the correct access to a system or have a smartcard. These are warning signs of potential privacy risks.
Automated Decision Making	Automated decisions only arise if 2 requirements are met. First, the decision has to be taken using personal information solely by automatic means. For example, if an individual applies for a personal loan online, the website uses algorithms and auto credit searching to provide an immediate yes / no decision. The second requirement is that the decision has to have a significant effect on the individual concerned.
Common Law Duty of Confidentiality	<p>This duty is derived from case law and a series of court judgements based on the key principle that information given or obtained in confidence should not be used or disclosed further except in certain circumstances:</p> <ul style="list-style-type: none"> <li>• Where the individual to whom the information relates has consented</li> <li>• Where disclosure is in the overriding public interest</li> <li>• Where there is a legal duty to do so, for example a court order</li> </ul>
Cyber Fraud	Crime committed via a computer with the intent to corrupt, disrupt or steal personal and financial information stored online for personal gain.
Data Protection Act 2018	This Act defines the ways in which information about living people may be legally used and handled. The main intent is to protect individuals against misuse or abuse

	<p>of information about them. The fundamental principles of DPA 2018 specify that personal data must be:</p> <ul style="list-style-type: none"> <li>• processed lawfully, fairly and transparently.</li> <li>• Collected for specified, explicit purposes (purpose limitation) adequate, relevant and limited to what is necessary (data minimisation).</li> <li>• accurate and where necessary kept up to date (accuracy).</li> <li>• Kept in an identifiable form for no longer than is necessary (storage limitation).</li> <li>• Processed in a manner that ensure appropriate security (integrity and confidentiality)</li> </ul> <p>The Act also requires organisations to be able demonstrate compliance with the principles (accountability).</p>
Direct Marketing	<p>This is “junk mail” which is directed to particular individuals. The mail which are addressed to “the occupier” is not directed to an individual and is therefore not direct marketing.</p> <p>Direct marketing also includes all other means by which an individual may be contacted directly such as emails and text messages which you have asked to be sent to you.</p> <p>Direct marketing does not just refer to selling products or services to individuals, it also includes promoting particular views or campaigns such as those of a political party or charity.</p>
European Economic Area (EEA)	The European Economic Area comprises of the EU member states plus Iceland, Liechtenstein and Norway
Explicit consent	Express or explicit consent is given by a patient agreeing actively, usually orally (which must be documented in the patients casenotes) or in writing, to a particular use of disclosure of information.
General Data Protection Regulation (EU) 2016/679 Principles of Lawful Processing of Personal Identifiable Information	<p>The GDPR requires that data controllers ensure personal data shall be:</p> <ol style="list-style-type: none"> <li>a) processed lawfully, fairly and in a transparent manner in relation to individuals</li> <li>b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or</li> </ol>

	<p>statistical purposes shall not be considered to be incompatible with the initial purposes</p> <p>c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed</p> <p>d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay</p> <p>e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals</p> <p>f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures</p>
IAA (Information Asset Administrator)	There are individuals who ensure that policies and procedures are followed, recognise actual or potential security incidents, consult their IAO on incident management and ensure that information asset registers are accurate and up to date. These roles tend to be system managers
IAO (Information Asset Owner)	These are senior individuals involved in running the relevant service/department. Their role is to understand and address risks to the information assets they 'own' and to provide assurance to the SIRO on the security and use of those assets. They are responsible for providing regular reports regarding information risks and incidents pertaining to the assets under their control/area.
Implied consent	Implied consent is given when an individual takes some other action in the knowledge that in doing so he or she has incidentally agreed to a particular use or disclosure of information, for example, a patient who visits the hospital may be taken to imply consent to a consultant consulting his or her medical records in order to assist diagnosis. Patients must be informed about this and the purposes of disclosure and also have the right to object to the disclosure.

Information Assets	Information assets are records, information of any kind, data of any kind and any format which we use to support our roles and responsibilities. Examples of Information Assets are databases, systems, manual and electronic records, archived data, libraries, operations and support procedures, manual and training materials, contracts and agreements, business continuity plans, software and hardware.
Information Risk	An identified risk to any information asset that the Trust holds. Please see the Information Risk Policy for further information.
Personal Data	Any information relating to an identifiable natural person (data subject), identified either directly or indirectly by:  Name, identification number, location data, online identifier, one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
Privacy and Electronic Communications Regulations 2003	These regulations apply to sending unsolicited marketing messages electronically such as telephone, fax, email and text. Unsolicited marketing material should only be sent if the requester has opted in to receive this information.
Privacy Invasive Technologies	Examples of such technologies include, but are not limited to, smart cards, radio frequency identification (RFID) tags, biometrics, locator technologies (including mobile phone location, applications of global positioning systems (GPS) and intelligent transportation systems), visual surveillance, digital image and video recording, profiling, data mining and logging of electronic traffic. Technologies that are inherently intrusive, new and sound threatening are a concern and hence represent a risk
Pseudonymisation	This is also sometimes known as reversible anonymisation. Patient identifiers such as name, address, date of birth are substituted with a pseudonym, code or other unique reference so that the data will only be identifiable to those who have the code or reference.
Records Management Code of Practice for health and social care records 2016	Is a guide to the required standards of practice in the management of records for those who work within or under contract to NHS organisations in England. This also includes public health functions in Local Authorities and Adult Social Care where their is joint care provided within the NHS.

	It is based on current legal requirements and professional best practice. The code of practice contains an appendix with retention schedules for a care records, business and corporate records.
Retention Periods	Records are required to be kept for a certain period either because of statutory requirement or because they may be needed for administrative purposes during this time. If an organisation decides that it needs to keep records longer than the recommended minimum period, it can vary the period accordingly and record the decision and the reasons behind. The retention period should be calculated from the beginning of the year after the last date on the record. Any decision to keep records longer than 30 years must obtain approval from The National Archives.
Senior Information Risk Owner (SIRO)	This person is an executive who takes ownership of the organisation's information risk policy and acts as advocate for information risk on the Board
Special Category Data	This means personal data revealing: <ul style="list-style-type: none"> <li>A. Concerning health, sex life or sexual orientation</li> <li>B. Racial or ethnic origin</li> <li>C. Political opinions</li> <li>D. Religious or philosophical beliefs</li> <li>E. Trade union membership</li> <li>F. Genetic data</li> <li>G. Biometric data</li> <li>H. Data concerning health</li> <li>I. Data concerning sex life or sexual orientation.</li> </ul>