NHS
Salford
Clinical Commissioning Group

Data Protection Impact Assessment (PIA) Proforma

Reference: LC25-19 Footfall
PIA Title: [FootFall – a Salford-wide Primary Care Digital Access Solution]
Version: [Final]
Date: [January 2020]

DOCUMENT CONTROL PAGE	
Title	Data Protection Impact Assessment Proforma
Version	2
Date	April 2018
Review	April 2020

Why do I need to complete a Data Protection Impact Assessment?

Data protection impact assessments (DPIAs) help organisations identify, assess and mitigate or minimise privacy risks with data processing activities. They're particularly relevant when a new data processing process, system or technology is being introduced.

DPIAs also support the accountability principle, as they help organisations comply with the requirements of the Data Protection Regulation and demonstrate that appropriate measures have been taken to ensure compliance.

A DPIA is a proforma or risk assessment which asks questions about the process or new system based on data quality / data protection / information security and technology.

Please note the template is constantly being changed / updated to meet new requirements so always make sure you use the latest version.

When do I complete a Data Protection Impact Assessment?

If you are doing any of the following:

GDPR introduces a new obligation to do a DPIA before carrying out types of processing likely to result in high risk to individuals' rights and freedoms.

- setting up a new process whether you are using personal confidential data (PCD) or not, then a DPIA should be completed and filed with the project paperwork
- changing an existing process which changes the way personal confidential data is used
- procuring a new information system which holds personal confidential data

They must be completed as early as possible to ensure risks can be identified and mitigated to an acceptable level.

Who needs to complete a Data Protection Impact Assessment?

It is the Information Asset Owners responsibility to ensure this is completed and submitted. They can delegate this task to an Information Asset Administrator (IAA) / Project Manager and or suppliers of a system / asset.

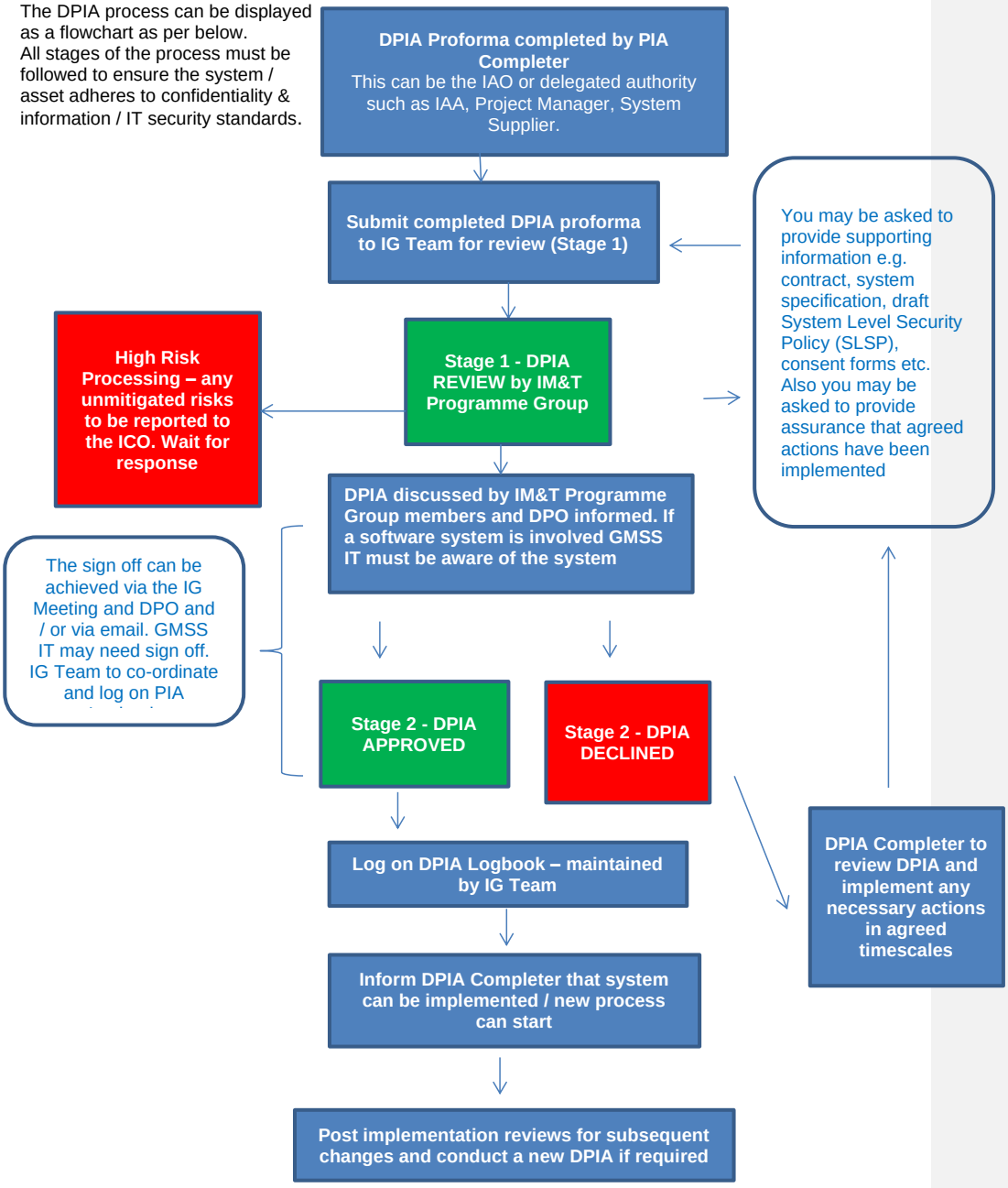
DPIA Process Flowchart

Please complete each section (where applicable) with as much information as possible. For example, a key piece of information is who the Information Asset Owner and Information Asset Administrator will be for a system / asset.

The following flowchart highlights the steps once the DPIA has been completed until either approval and / or rejection decision has been reached.

Data Protection Impact Assessment Process Flowchart

The DPIA process can be displayed as a flowchart as per below.
All stages of the process must be followed to ensure the system / asset adheres to confidentiality & information / IT security standards.



Important

By completing this Data Protection Impact Assessment, all parties associated with the DPIA agree to adhere to the Data Security & Protection Toolkit requirements and have Data Security and Information Security Policies in place as follows:

- System Level Security Policy including Business Continuity Plan
- Data Protection Procedure/Policy
- Completion of Data Security mandatory training
- Incident Reporting Procedures
- Safe Transfers of Information Procedure
- Information Asset Register
- Data Flow Mapping Register

The list above is not exhaustive.

In the event of an incident and failure to have the above may incur a larger monetary penalty being levied upon you by the Information Commissioners Office (ICO).

Screen 1: PIA Completed by:

Organisation	Name	Date	Signature
Salford Primary Care Together		11/11/2019	
Silicon Practice		11/11/2019	

For completion by: IG/Approval Group

Approved – no actions required	☒	Click here to enter a date.
Approved with action plan	☐	Click here to enter a date.
Declined (give reason)	☐	Click here to enter text. Click here to enter a date.

Screen 2: Basic Information

PIA Completer Name:*(please note this can be Project Manager / IAO / IAA or whoever has been requested to complete the proforma):*	SPCT
Department:	Salford Primary Care Together
Email:	
Telephone No.:	
New System / Process Name:	FootFall
New System Supplier Name: **(if applicable):**	Silicon Practice
Date System due to go live (if applicable):	TBC
Project Proposal / Purpose for completing DPIA:	To roll out a city wide online web based system
Link to any wider initiative: *(if applicable)*	Enter links to any wider initiatives if applicable
Information Technology involvement	List any applicable electronic systems/software to this initiative (current and/or new):

<table>
<tr><td></td><td>
<table>
<tr><th>System name</th><th>Used by e.g. organisation and dept.</th><th>Parties/system supplier</th></tr>
<tr><td>Footfall</td><td>GP Practices</td><td>Silicon Practice</td></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td></tr>
</table>
</td></tr>
<tr><td>Are any other organisations are involved in this initiative?</td><td>All GP Practices in Salford</td></tr>
<tr><td>Confirm all relevant organisations have or are working towards cyber essentials</td><td>
<table>
<tr><th>Organisation/Parties/ system supplier</th><th>Cyber essentials Y/N
Working towards/cyber compliance defined under terms of contract</th></tr>
<tr><td>Silicon to confirm</td><td>Y</td></tr>
<tr><td></td><td></td></tr>
<tr><td></td><td></td></tr>
<tr><td></td><td></td></tr>
<tr><td></td><td></td></tr>
</table>
</td></tr>
<tr><td>Is this initiative in line with or achieving national or local guidance/
strategy or mandate?</td><td>If yes give details

FootFall is an innovative design creating a truly extraordinary and comprehensive digital practice. It is aligned perfectly to the needs of all the teams within a GP Practice, such as Receptionists, Practice Nurses, GPs, Administrators and Medical Secretaries. It has been specifically designed to provide digital access for the population to the services typically provided by GP Practices, and as a source of advice and information.

This is a transformative and innovative proposal, radically improving the efficiency and productivity of GP Practice operations.

Silicon Practice is listed on NHS England website - Dynamic Purchasing System Framework – Online Consultations – Approved Suppliers
https://www.england.nhs.uk/digitaltechnology/digital-primary-care/commercial-procurement-hub/dynamic-purchasing-system/

As required by the NHS Long Term Plan (2019) an innovative digital technology solution that provides convenient ways for patients to access advice and care.</td></tr>
</table>

Screen 3: Screening Question

Documenting here which of the screening questions are applicable to your initiative will help to draw out the particular privacy considerations that will help formulate your risk register later in the template

		Yes	No	Unsure	**Comments** *Document initial comments on the issue and the privacy impacts or clarification why it is not an issue*
a)	Is the information about individuals likely to raise privacy concerns or expectations e.g. health records, criminal records or other information people would consider particularly private?	☐	☒	☐	Click here to enter text.
b)	Will the initiative involve the collection of new information about individuals?	☒	☐	☐	Click here to enter text.
c)	Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?	☐	☒	☐	Click here to enter text.
d)	Will the initiative require you to contact individuals in ways which they may find intrusive[1]?	☐	☒	☐	Click here to enter text.
e)	Will the information about individuals be disclosed to organisations or people who have not previously had routine access to the information?	☐	☒	☐	The patients completed form is sent to a secure dashboard for the GP Practice to process and in some cases respond. This dashboard is encrypted, requires a login and is restricted to the GP Practice IP address. Responses to the patient are sent to an email address provided in the original request. No personal or sensitive information is sent in the email. The patient must select the link in the email and enter their Date of Birth for verification; the response from the practice is viewed in the browser. The number of attempts is limited to 3, the link in the email will also 'self-destruct' after 7 days.

					On occasion it may also be viewed by internal staff providing helpdesk support.
f)	Does the initiative involve you using new technology which might be perceived as being intrusive? e.g. biometrics or facial recognition	☐	☒	☐	Click here to enter text.
g)	Will the initiative result in you making decisions or taking action against individuals in ways which can have a significant impact on them?	☐	☒	☐	Click here to enter text.
h)	Will the initiative compel individuals to provide information about themselves?	☐	☒	☐	Click here to enter text.

If you answered **YES or UNSURE** to any of the above you need to continue with the Data Protection Impact Assessment.

***Sign off if no requirement to continue with Privacy Impact Assessment*:**	
Confirmation that the responses to a – h above is NO and therefore there is no requirement to continue with the Privacy Impact Assessment	
Agreed by:	Click here to enter name of group or individual(s).

Screen 4: Contact Information

Project Management Details	
Project Manager:	
Project Manager Email:	
Project Manager Telephone No.:	
Information Asset Owner (IAO) Details	
IAO Name:	Each GP Practice
IAO Title:	Click here to enter text.
IAO Department:	Click here to enter text.
IAO Email:	Click here to enter text.
IAO Telephone Number:	Click here to enter text.
Information Asset Administrator (IAA) Details	
IAA Name:	Each GP Practice
IAA Title:	Click here to enter text.
IAA Department:	Click here to enter text.
IAA Email:	Click here to enter text.
IAA Telephone Number:	Click here to enter text.

Commented [JW1]: GP Surgery- who has overall responsibility within the practice for managing risks to personal information and business critical information?

Commented [JW2]: GP Surgery- who look after the day to day management?

Screen 5: Personal Confidential Data Items

	Yes	No	If Yes complete the rest of the form. If No go to screen 7
Is the project collecting Personal Confidential Items	☒	☐	Click here to enter text.

What data items are being processed e.g. for collection, storage, use and deletion: If there is a chart or diagram to explain please attach as an appendix			
Data Item	**Description**	**Specific data item(s)**	**Justification** Reason that the data items(s) are needed – this must stand up to scrutiny for Caldicott justification
Personal details	Information that identifies the individual and their personal characteristics	Check all that apply: ☑ Forename(s) ☑ Surname ☑ Address ☑ Postcode ☑ Date of Birth ☐ Age ☑ Gender ☐ Physical description ☑ Home Telephone Number ☑ Mobile Telephone Number ☑ Other Contact Number ☐ Email address ☑ GP Name and Address ☑ Legal Representative Name (Next of Kin) ☑ NHS Number ☐ National Insurance Number ☐ Photographs/Pictures of persons ☐ Other – if this is ticked please list 'Other' personal data items to be processed below: See attached	Click here to enter text.
Physical or mental health or condition	Information relating to the individuals physical or mental health or	☐ Yes ☐ No	Click here to enter text.

What data items are being processed e.g. for collection, storage, use and deletion: If there is a chart or diagram to explain please attach as an appendix			
Data Item	**Description**	**Specific data item(s)**	**Justification** Reason that the data items(s) are needed – this must stand up to scrutiny for Caldicott justification
	condition. NB. For mental health this would include the mental health status i.e. whether detained or voluntary under the Mental Health Act.	☐ Not applicable List any data items below or attach as an appendix: Click here to enter text.	
Sexual identity and life	Information relating to the individuals sexual life	☐ Yes ☐ No ☐ Not applicable List any data items below or attach as an appendix: Click here to enter text.	Click here to enter text.
Family lifestyle and social circumstances	Information relating to the family of the individual and the individuals lifestyle and social circumstances	☐ Marital/partnership status ☐ Carers/relatives ☐ Children/dependents ☐ Social status e.g. housing ☐ Not applicable ☐ Other - please specify below: Click here to enter text.	Click here to enter text.
Offences including alleged offences	Information relating to any offences committed or alleged to have been committed by the individual	☐ Yes ☐ No ☐ Not applicable List any data items below or attach as an appendix: Click here to enter text.	Click here to enter text.
Criminal proceedings, outcomes and sentences	Information relating to criminal proceedings outcomes and sentences regarding the individual	☐ Yes ☐ No ☐ Not applicable List any data items below or attach as an appendix:	Click here to enter text.

What data items are being processed e.g. for collection, storage, use and deletion: If there is a chart or diagram to explain please attach as an appendix			
Data Item	**Description**	**Specific data item(s)**	**Justification** Reason that the data items(s) are needed – this must stand up to scrutiny for Caldicott justification
		Click here to enter text.	
Education and training details	Information which relates to the education and any professional training of the individual	☐ Education/training ☐ Qualifications ☐ Professional training ☐ Not applicable ☐ Other - please specify below: Click here to enter text.	Click here to enter text.
Employment details	Employment and career history	☑ Employment status ☐ Career details ☐ Not applicable ☐ Other - please specify below: Click here to enter text.	Click here to enter text.
Financial details	Information relating to the financial affairs of the individual	☐ Income ☐ Salary ☐ Benefits ☐ Not applicable ☐ Other – please specify below: Click here to enter text.	Click here to enter text.
Religious or other beliefs of a similar nature	Information relating to the individuals religion or other beliefs	☐ Yes ☐ No ☐ Not applicable List any data items below or attach as an appendix: Click here to enter text.	Click here to enter text.
Trade union membership	Information relating to the individuals membership of a trade union	☐ Yes ☐ No ☐ Not applicable	Click here to enter text.

What data items are being processed e.g. for collection, storage, use and deletion:
If there is a chart or diagram to explain please attach as an appendix

Data Item	Description	Specific data item(s)	**Justification** Reason that the data items(s) are needed – this must stand up to scrutiny for Caldicott justification
		List any data items below or attach as an appendix: Click here to enter text.	

You must confirm that the data items you have ticked above are relevant and necessary to your project and there is a justified reason for it –if they are not you must amend the above selections to remove those items not relevant/necessary

Confirm ☐

Screen 6: Legal Basis for Processing the Data

Is the initiative delivering for Direct Care?

The definition of direct care is: 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*
- *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

☒ **Yes (go to Q2)** ☐ **No (go to Q1)** ☐ **N/A (go to screen 7)**

1a. If not Direct care, what is it delivering and how is the consent being obtained 1b. What is the legal basis that permits you to carry this out for indirect care?	Indirect care • Commissioning ☐ • Monitoring Health and social care ☐ • Public health ☐ • Research ☐ • Other ☐ specify …… Legal basis: • Explicit consent ☐ • Section 251 ☐ • Other legal gateway (please state) ☐ Click here to enter text.
2. What are the arrangements for individual's to either *object* to their information being shared for *direct care* or to *opt-out* of the initiative for *indirect care* once they have been provided with appropriate communication about it?	The individual logs in to request for certain items identifiable information is not shared.

Informing individuals: How have patients and / or staff been informed of the data collection and processing?	Please state: Silicon Practice have a privacy notice on their front end screen

Information Sharing within UK:

Will personal confidential data be shared with any other organisation?

If yes, please state who the information will be shared with and how

☐ Yes ☒ No

From Originator Organisation:	Data sent to via:	To Receiving Organisation:

Is the information from receiving organisation sent back to originating organisation. If yes, please state how the information is transferred back:

From Receiving Organisation:	Data sent back via:	To originating organisation:

Information Sharing outside the UK:

Will Personal Confidential Data be sent outside the UK?

☐ Yes

☒ No

If yes, please state who the data will be sent to and how?

☐ Yes

Will Personal Confidential Data be sent outside the European Economic Area (EEA)?

☐ No

If yes, please state who the data will be sent to and how?

☐ Yes

Have data protection checks been undertaken to ensure that the non EEA country has adequate data protection / information security? If yes, please state what checks have been made: **Sending data to the USA**	☐ No ☐ Yes ☒ No

Screen 7: Asset / System Information

ICO Notification: If a system is being used, is the Supplier registered with the Information Commissioners Office (ICO). If yes, please state their registration number:	☐ Yes ☐ N/A ☐ No Z9216576
IG Toolkit: Has the Supplier / Third party completed an Data Security and Protection Toolkit (DS&P) Assessment & that has been internally/externally audited and/or has ISO27001 accreditation? If so, which version and to what level? Please provide evidence.	Data Security and Protection Toolkit completed: ☒ Yes ☐ No DS&P Toolkit audited ☒ Yes ☐ No ISO 27001 Accreditation ☐ Yes ☒ No Evidence: The Data Security and Protection Toolkit was last completed in April 2019 resulting in a score of Satisfactory. An internal audit was subsequently completed resulting in a gap analysis and action plan. We will be submitting the next Toolkit before April 2020. We are currently working towards ISO27001 accreditation and hope to have this is the first quarter of 2020.
Contract: Has the supplier (if applicable) signed the relevant contract (containing the Information Governance clauses) e.g. NHS E contract / SLA with IG Clause. If yes, please state which contract type they have signed up to:	☒ Yes ☐ No ☐ N/A Supplier on Framework

Asset / System Operation: Does the asset use privacy invasive technologies for staff and / or patients? See **Glossary** for advice	☐ Yes ☒ No
If yes, please state the technology being used:	Click here to enter text.
Will the asset / system process new / different personal confidential data items which have not been processed previously?	☐ Yes ☐ No
If yes, please state the new personal confidential data items to be processed:	Click here to enter text.
Will the asset / system involve new or changed identity authentication requirements that may be intrusive for staff and / or patients?	☐ Yes ☒No
If yes, please state the new identity authentication requirements:	Click here to enter text.
Marketing: Will the asset / system send marketing messages by electronic means?	☐ Yes ☒No
If yes, please state what you are intending to send for marketing purposes:	
Have individuals been informed of the marketing and the option to opt in?	☐ Yes ☐ No

	Click here to enter text. **N/A**
Automated Decision Making: Is automated decision making to be used within the asset / system? If yes, please describe this process and reason for it	☐ Yes ☒ No Click here to enter text.

Screen 8: System Security and Functions – only to be completed for systems

Pseudonymisation / Anonymisation: Can personal confidential data be anonymised or pseudonymised using the system / asset?	☒ Yes ☐ No
Data Quality: How will the personal confidential data be kept up to date and checked for accuracy?	The personal information that is processed through FootFall is information that a patient has submitted using one of the forms and therefore the patient is responsible for the accuracy of said information. As for keeping the data up to date, it is transactional and not static and therefore does not require review in this fashion.
Access: Who will have access to the system and the personal confidential data? How will levels of access be decided.	Silicon Practice employees will have access to the system for the purpose of maintenance and support.
Auditing: Is there an audit trail for the system?	☒ Yes ☐ No
Storage of data: Where will the system information be stored securely?	☐ Within a paper based system stored securely ☒ Within a system / application stored on secure network ☐ Within a database / spreadsheet stored securely on network ☐ Other Click here to enter text.
Retention: What are the retention periods for the information processed in the system?	90 days for retention period for data backups and 2 years for data stored on the server. This is in line with the Records Management Code of Practice for Health and Social Care 2016.
Disposal: How will the personal confidential data be disposed of when this is no longer required?	The data backups and servers automatically destroy electronic data upon the expiration of the retention period.

Commented [JW3]: The practice will need to add to this answer to reflect who will have access their end.

Training: Each party to confirm that information governance training is in place and all staff with access to personal data have had up to date training	☒ Yes ☐ No

Commented [JW4]: All Silicon Practice staff have completed information governance training and this is renewed annually.

Additional Comments

Do you wish to supply additional comments about the system / asset? If yes please input comments in box:	☐ Yes ☐ No Click here to enter text.

Signed off by:

Organisation	Name	Date	Signature
Salford Primary Care Together		10.1.20	
Salford CCG	IM&T Programme Group	21/01/2020	R A Quinn

Glossary of Terms

Item	Definition
Personal Data	This means data which relates to a living individual which can be identified: A) from those data, or B) from those data and any other information which is in the possession of, or is likely to come into the possession of, the data controller. It also includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual
Special Category Data	This means personal data consisting of information as to the: race; ethnic origin; politics; religion; trade union membership; genetics; biometrics (where used for ID purposes); health; sex life; or sexual orientation
Direct Marketing	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. 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. 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.
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.
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.
SIRO (Senior Information Risk Owner)	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
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.
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
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.
Explicit consent	Express or explicit consent is given by a patient agreeing actively, usually orally (which must be documented in the patients case notes) or in writing, to a particular use of disclosure of information.
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.
Pseudonymity	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.
Information Risk	An identified risk to any information asset that the Trust holds. Please see the Information Risk Policy for further 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
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.
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.
Records Management: NHS Code of Practice	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. It is based on current legal requirements and professional best practice. The code of practice contains an annex with a health records retention schedule and a Business and Corporate (non-health) records retention schedule.
Data Protection Legislation	This Legislation defines the ways in which information about living people may be lawfully used and handled. The aim is to protect individuals against misuse or abuse of information about them. The Act defines the ways in which information about living people may be lawfully used and handled. The aim is to protect individuals against misuse or abuse of information about them. The 8 principles of the Act state The fundamental principles of DPA 1998 specify that personal data must: with those purposes. loss, destruction or damage. unless that country or territory protects the rights and freedoms of the data subjects.
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. 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.