

Data Protection, General Data Protection Regulations (GDPR) and Confidentiality Policy

IG02

Versions:	V4
V1 issued	September 2009
V2.5 issued	August 2013
V3 reviewed and reissued:	February 2015
V3 Date approved	January 2019
V3 approved by:	Policy Approval Group
V3 Ratified by:	Performance Committee
V3 Date ratified:	January 2019
Document Lead	Data Protection Officer
Lead Director	Medical Director / Caldicott Guardian
Date issued:	February 2019
Review date:	February 2024 subject to annual review in light of any legislative changes
Target audience:	All Data/Information Handlers
Relevant Policies	<ul style="list-style-type: none">• Information Governance & Framework Policy• Information and Information Systems Security Policy• Over-arching Data Sharing Protocol• Reporting of security / confidentiality breaches/incidents• Access to Health Records• Subject Access Requests• Information Asset Management policy• Standard Operating Procedure for the Management of Information Governance Serious Incidents Requiring Investigation (SIRI)

Document Control Sheet

Document Lead/Contact:	Data Protection Officer
Version	4
Status	Final
Date Equality Impact Assessment completed	26 th November 2018
Issue Date	February 2019
Review Date	2024 (in line with national opt out programme and developments with Brexit)
Distribution	Please refer to the intranet version for the latest version of this policy. Any printed copies may not necessarily be the most up to date
Key Words	Data Protection, Confidentiality, GDPR
Dissemination plan	This document will be disseminated via policy leads and the communications team, management cascade using 4policies and the IG Group

Version history

Version	Date	Author	Status	Comment – include reference to Committee presentations and dates
V2.5	August 2013	J. Stretton	Draft	
V3	February 2015	J. Stretton		Reviewed.
V4	December 2018	R. Samuel	FINAL	To include GDPR implementation and all the associated changes. Changed title to include 'Confidentiality' (to reduce duplication and volume of IG related policies). To be reviewed in 2020 due to national data opt-out and political decisions around Brexit.
V4	June 2020	R. Samuel	Amendment	Updated DPIA template and IGA / NHS X section
V4	January 2021	R. Samuel	Amendment	Updated DPIA template



**The Shrewsbury and
Telford Hospital**
NHS Trust

Contents

1. Policy on a page.....	5
2. Document Statement	6
3. Overview.....	6
4. Duties and Responsibilities	7
5. General Data Protection Regulation (EU) 2016//679 (DPA Principles).....	7
6. Definition of data.....	9
7. Legal Basis for Processing Identifiable Data.....	10
8. Consent & Opt Out.....	13
9. Ensuring Information is Secure and Confidential.....	13
10. Data Breaches	18
11. Contracts	19
12. Documentation	20
13. Data Protection by design and default.....	21
14. International Transfers.....	22
15. Exemptions	22
16. Implementation and Training.....	23
17. Monitoring Compliance.....	23
18. Equality Impact Assessment	24
19. Consultation process.....	24
20. Associated documents	24
21. Other Legislation and External References.....	24
22. Appendix 1	29

1. Policy on a page

The Data Protection, GDPR and Confidentiality Policy has been developed to provide awareness and guidance to The Shrewsbury and Telford Hospital NHS Trust (SaTH) staff on the impact of the new General Data Protection Regulation (GDPR) that was implemented within the European Union (EU) on 25 May 2018.

The policy includes:

- a) How it is every employees' responsibility to use personal and confidential information in line with the principles of the Data Protection Act 2018 (DPA) and the General Data Protection Regulation (GDPR).
- b) How it is every employees' responsibility to ensure all personal data and where necessary corporate information is protected and kept secure.
- c) The accountability and responsibilities of specific staff roles in the organisation.
- d) Definitions of Personal Data.
- e) Definitions of Special Category *formerly* 'sensitive' data.
- f) Guidance on the different 'legal basis' for processing personal information.
- g) Using and disclosing confidential information.
- h) Using and disclosing Corporate and Business Information.
- i) Information Sharing / Data Flow
- j) Information Security and Confidentiality Breaches, what should be reported.
- k) Data Protection Impact Assessments (DPIA) required when implementing new systems or processes
- l) The General Data Protection Regulation principles *formerly* DPA 1998 Principles.
- m) Individual's rights in relation to their personal data under the GDPR and the use of privacy notices
- n) The importance of the mandatory IG Training.
- o) Information Assets

2. Document Statement

The DPA, the GDPR and the requirements of confidentiality underpin and support the *Information Governance (IG) Framework* for the management of all data from which individuals can be identified. It is essential that all staff and contractors of SaTH are fully aware of their personal responsibilities for protecting personal, confidential information which they may come into contact with.

SaTH recognises the importance of reliable information, both in terms of the clinical management of individual patients and the efficient management of services and resources.

SaTH also recognises the duty of confidentiality owed to patients, families, carers, staff, volunteers and business partners with regard to all ways in which it processes, stores, shares and disposes of information.

The aim of the policy is to ensure that all staff have a clear understanding of their obligations with regard to any information they come into contact with in the course of their work and to provide assurance to the Trust Board by having in place appropriate processes, rules and guidelines to ensure such information is dealt with/handled legally, efficiently and effectively.

SaTH has established, implemented and will continue to maintain procedures linked to this policy to ensure compliance with the requirements of the Data Protection Act 2018 and the GDPR and other associated/related legislation, and contractual responsibilities to support the assurance standards of the Data Security and Protection Toolkit (DSP Toolkit).

This policy supports SaTH in its role of a provider of healthcare services as a data controller and data processor and supports the safe information/data sharing of with third party/partner agencies.

3. Overview

This policy must be followed by all staff who are employed by or on behalf of the Trust including those on temporary or honorary contracts, secondments, volunteers, bank/temporary/locum staff, Governing Body members, students and any staff working on an individual contractor basis or who are employees for an organisation contracted to provide services to SaTH. The policy is applicable to all areas of the organisation and adherence should be included in all contracts for outsourced or shared services. There are no exclusions.

This policy covers:

All aspects of information within the organisation, including (but not limited to):

- Patient / Service User information.
- Personnel / Staff information.
- Organisation and business sensitive information.
- Structured and unstructured record systems – paper and electronic.
- Photographic images, digital, text or video, audio recordings including CCTV.
- All information systems purchased, developed and managed by/or on behalf of the organisation.

- Hardware and Software
- SaTH information held on paper, mobile storage devices, computer, laptops, tablets, mobile phones and cameras.

The processing of all types of information, including (but not limited to):

- Organisation, adoption or alteration of information.
- Retrieval, consultation, storage/retention or use of information.
- Disclosure, dissemination or otherwise making available information for clinical, operational or legal reasons.
- Alignment, combination/linkage, blocking, erasing or destruction of information.

The Trust recognises the changes introduced to information management as a result of the *GDPR 2018, Data Protection Act 2018, the Health and Social Care Act 2012* and the *Health and Social Care (Safety and Quality) Act 2015* and will continue to work with national bodies and regulators to ensure the continuing safe use of information to support services and clinical care.

Failure to adhere to this policy may result in disciplinary action and where necessary referral to the appropriate regulatory bodies including the police and professional bodies.

4. Duties and Responsibilities

There are a number of key information governance roles and bodies that the Trust needs to have in place as part of its *Information Governance (IG) Framework*, these are:

- Senior Information Risk Owner (SIRO)
- Caldicott Guardian
- Information Governance Manager
- Data Protection Officer (DPO)
- Information Asset Owner (IAO)
- Information Asset Administrator (IAA)
- Information Governance Group
- All employees

The accountability and responsibilities are set out in more detail in the IG Framework and Strategy and the Information Asset Management policy, which may be read in conjunction with this policy.

5. General Data Protection Regulation (EU) 2016//679 (Formerly the DPA Principles)

The GDPR was implemented on the 25 May 2018 and it forms part of the data protection regime in the UK, together with the new Data Protection Act 2018. The GDPR requires that data controllers ensure personal data shall be:

- Processed lawfully, fairly and in a transparent manner in relation to individuals.

- 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 statistical purposes shall not be considered to be incompatible with the initial purposes.
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- 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.
- 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 in so far as the personal data may 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.
- Processed in a manner that ensures appropriate security of the unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

It is important to note that the Regulation specifies that:

- Organisations are accountable for how they handle personal data and need to develop and maintain adequate policies, procedures, processes and systems to fulfil this role.
- Data processors can be held liable for breaches
- All actual information breaches must be reported via the Data Security and Protection Toolkit (DSPT) (to the Information Commissioner Office (ICO)) within 72 hours of becoming known and the Trust is required to have a local record of all near miss / actual data breaches.
- the penalty for breach of the Regulations is now capped at a maximum of €20,000,000 or 4% of the turnover of an organisation
- Organisations must employ the privacy by design approach to activities involving personal data. A Data Protection Impact Assessment is required for any project where personal data will be processed or flow or it is otherwise anticipated to have a high privacy risk
- Fair processing notices (privacy notices) must transparently explain how personal data is used and the rights of the data subject
- Organisations outside of the EU are required to follow the principles of the Regulations if their customers/clients are based within the EU
- Data subjects have the new right to erasure, data portability, review of automated decision making and profiling, to request their personal data are removed when an organisation is retaining them beyond a reasonable or defined time period
- Organisations must keep a record of processing activities
- Put written contracts in place with organisations that process personal data for the Trust
- Implement appropriate security measures – Refer to the Trusts Information and Information Systems Security Policy
- Appointment of a Data Protection Officer, which the Trust has in place.

The Data Protection Bill 2017 includes the national derogations of the GDPR and the implementation of Law Enforcement Directive (EU) 2016/680:

- The processing of personal data for law enforcement
- It defines which organisations are considered Public Authorities
- Process of reporting and potential consequences of data breaches
- The processing of personal data relating to children under the age of 13 years and the ability to seek the consent of children aged 13 years or older
- Role and powers of ICO and provision to charge fees
- Conditions for processing
- Allowances for complaints and compensation, which can now include financial loss, distress and other adverse effects
- Establishes new criminal offences: “knowingly or recklessly to re-identify information that is de-identified personal data”, data theft, unlawful obtaining of personal data and alteration of personal data in a way to prevent it being disclosed
- Exemptions to the provisions of GDPR

6. Definition of data

The GDPR defines personal data as:

- Relating to a living human being who can be directly or indirectly identified.
- Identifiers include ID numbers, location data, physical, psychological, genetic, mental factors, this may include (but is not limited to):
 - Name
 - Date of Birth
 - Postcode
 - Address
 - National Insurance Number
 - Photographs, digital images etc.
 - NHS Number
 - Hospital Number
 - Date of Death
 - Passport Number
 - Online Identifiers and location data (such as MAC, IP addresses and mobile device ID's)

Definition of Special Categories data

Categories of information are classified as special categories of personal data and require additional safeguards '*formerly sensitive data*' when sharing or disclosing this information in line with guidance and legislation. This includes (but is not limited to):

- Concerning health, sex life or sexual orientation.
- Racial or ethnic origins.
- Trade union membership.
- Political opinions.
- Religious or philosophical beliefs.
- Genetic / Biometric data.

Definition of Corporate Information

Corporate information includes:

- Trust Board and meeting papers and minutes.
- Tendering and contracting information.
- Financial and statistical information.
- Project and planning information.

Corporate information could be accessible through the Freedom of Information Act (FOIA) either from the Trust responding to a request for information or through making information accessible via the Trust's website. Where any corporate information has a duty of confidence attached to it the information may be exempt from release. Additionally, other exemptions of the FOIA could restrict release of certain corporate information.

Definition of 'Direct' Patient Care

The Caldicott Report (1997) defined direct patient care 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 individual's 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 professional and their team with whom the individual has a legitimate relationship for their care".

The Trust must adhere to legislation and national guidance in relation to using Personal Confidential Data and recognises that such data can only flow where a clear legal basis enables this. Caldicott principle seven, which sets out that 'the duty to share information can be as important as the duty to protect patient confidentiality'.

7. Legal Basis for Processing Identifiable Data

To enable the Trust to identify the grounds for lawful processing (legitimising conditions, article 6) a data mapping exercise must be completed to:

- A Data Protection Impact Assessment (DPIA) may be required in order to demonstrate a legal basis for processing identifiable data.
- Identify what personal data is held, where it comes from and who it is shared with.
- Consider legal justification for these activities '*legal basis*'
- Where data is processed or used for another purpose for which it was obtained, explicit consent will be required.

Explicit consent is described in the GDPR as any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, through a statement or clear affirmative action, signifies agreement to the processing of their personal data

An overview of these considerations is provided within the Trust's Privacy Notices available on the organisations website.

There are six available lawful bases for processing. No single basis is 'better' or more important than the others – which basis is most appropriate to use will depend on the purpose and relationship with the individual. The six include:

1. Consent: the individual has given clear consent for you to process their personal data for a specific purpose.
2. Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.
3. Legal Obligation: the processing is necessary for you to comply with the law (not including contractual obligations).
4. Vital Interests: the processing is necessary to protect someone's life.
5. Public Task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.
6. Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

If you are processing special category data you need to identify both a lawful basis for general processing and an additional condition for processing this type of data.

In line with the GDPR, Personal data concerning health as a 'special category'; the most appropriate Article 9 condition for 'direct care' or 'administrative purposes' is:

9(2) (h) '... medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems...'

These conditions will also be the most appropriate basis for local admin purposes such as:

- Waiting list management
- Performance against national targets
- Activity monitoring
- Local clinical audit
- Production of datasets to submit for commissioning purposes and national collections.

Lawful basis for regulatory and public health functions – where the processing is necessary for the exercise of a mandated regulatory function, the most appropriate Article 6 and 9 conditions are:

6(1) (c) '...necessary for compliance with a legal obligation...' and:

9 (2) (j) '... necessary for reasons of public interest in the area of 'public health'... or ensuring high standards of quality and safety of health care and of medicinal products or medical devices...'

Information relating to criminal convictions and offences are not 'special categories' data, however the DPA does deal with this type of data in a similar way to special category data and sets out specific conditions providing lawful authority for processing it. Refer to Article 10 provisions as a basis for processing such data.

For purposes of safeguarding children and vulnerable adults, the following Article 6 and 9 conditions may apply:

6(1) (e)' ... for the performance of a task carried out in the public interest or in the exercise of official authority....' And

9(2)(b)'... is necessary for the purposes of carrying out the obligations and exercising the specific rights of the controller or of the data subject in the field of ... social protection law in so far as it is authorised by Union or Member State law...'

Lawful basis for employment purposes – the following condition for lawful processing will apply:

6(1)(e)'...for the performance of a task carried out in the public interest or in the exercise of official authority....'

For necessary processing of 'special categories', e.g. health data for employment purposes the following condition will apply:

9(2)(b)'... is necessary for the purposes of carrying out the obligations and exercising the specific rights of the controller or of the data subject in the field of employment... social protection law in so far as it is authorised by Union or member State law...'

7.1 Lawful basis for commissioning and planning purposes

Most national and local flows of personal data in support of commissioning are established as collections by NHS Digital either centrally, or for local flows by its Data Services for Commissioners Regional Offices (DSCRO). These information flows do not operate on the basis of consent for confidentiality or data protection purposes.

Where the collection or provision of data is a legal requirement, for example where NHS Digital is directed to collect specified data, and can require specified organisations to provide it, GDPR still needs to be complied with and the appropriate Article 6 condition for NHS Digital and the providers of the data is:

6(1) (c) '...necessary for compliance with a legal obligation...'

Commissioners may receive personal data in support of commissioning where confidentiality is set aside by provisions under the Control of Patient Information Regulations 2002, commonly known as 'section 251 support'. This support does not remove the need for GDPR compliance.

For GDPR compliance, the most appropriate Article 6 condition for disclosure by NHS Digital and for subsequent processing by commissioners in these circumstances is:

6(1) (e)' ... for the performance of a task carried out in the public interest or in the exercise of official authority....'

Although there is a move to the use of pseudonymised data for commissioning purposes, this data may constitute personal data under GDPR, so this condition continues to be applicable. As for 'direct care' the most appropriate Article 9 condition for commissioning purposes is:

9(2) (h) '... medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems...'

The commissioning of individual tailored services, or for example the approval of individual funding requests should operate on the basis of consent for confidentiality purposes provided the individual is informed or the sharing is otherwise within reasonable expectations. Again, Article 6(1) (e) is the most appropriate condition for GDPR purposes and common law consent practices do not need to be changed.

8. Consent & Opt Out

Where patient identifiable information is being processed for purposes other than 'Direct Care', there is an obligation to respect opt outs that have already been presented.

The Information Commissioners Office states that "The basic concept of consent, and its main role as one potential lawful basis (or condition) for processing, is not new. The definition and role of consent remains similar to that under the Data Protection Act 1998 (the 1998 Act). However, the GDPR builds on the 1998 Act standard of consent in several areas.

The GDPR sets a high standard for consent, but the biggest change is what this means in practice for consent mechanisms. You need clear and more granular opt-in methods, good records of consent, and simple easy-to-access ways for people to withdraw consent."

Alongside this, NHS Digital have developed a new service that allows patients to opt out of their confidential patient information being used for research and planning. All health and care organisations in England will be expected to comply with the national data opt-out policy by March 2020.

For further information on this area, please contact the Information Governance Office.

9. Ensuring Information is Secure and Confidential

General Principles

- The Trust regards all identifiable personal information relating to patients as confidential and compliance with the legal and regulatory framework will be achieved, monitored and maintained.
- The Trust regards all identifiable personal information relating to staff as confidential except for where national policy on accountability and openness requires otherwise.
- The Trust will establish and maintain policies and procedures to ensure compliance with the GDPR, Data Protection Act, Human Rights Act, The Common Law Duty of Confidentiality, Privacy and Electronic Communications Regulations, The Freedom of Information Act and Environmental Information Regulations and other related legislation and guidance.

- Awareness and understanding of all staff, with regard to responsibilities, will be provided with appropriate Data Security and Protection` training and awareness.
- Risk Assessment, in the form on Data Protection Impact Assessment, in conjunction with overall priority planning of organisational activity will be undertaken to determine appropriate, effective, confidentiality and data protection controls are in place.
- Where any disclosure of patient confidential data is made there must be a legal basis for doing so.

9.1 Using and Disclosing Confidential Patient Information for Direct Healthcare

Consent to disclose can usually be implied when the information sharing is needed for direct healthcare, however, this still requires that patients be informed about:

- The use and disclosure of their healthcare information and records.
- The choices that they have and the implications of choosing to limit how information may be used or shared.
- The breadth of the sharing necessary when care is to be provided by partner agencies and organisations.
- The potential use of their records for the clinical governance audit of the care they received.
- The Privacy Notice available on the organisations website outlining what information will be shared, the purpose of this, how long data will be retained, the rights of the data subject and what security measures are in place to protect confidentiality.
- If not for direct care then explicit consent or some other legal basis must be present to enable sharing.

9.2 Using and Disclosing Confidential Staff Information

Processing of personal data where the information sharing is needed for direct communications related to their role, salary payment and pension arrangements, is lawful. Staff should be made aware that disclosures may need to be made for legal reasons, the professional regulators bodies and in certain categories of freedom of information requests where the public interest in disclosure is deemed to override confidentiality considerations.

Using staff information for other purposes must be subject to explicit consent being granted unless another legal basis permits this.

9.3 Using and Disclosing Corporate and Business Information

All staff should consider all information which they come into contact with through the course of their work as confidential and its usage and any disclosure would be in line with agreed duties and for authorised work purposes.

Corporate information could be accessible through the Freedom of Information Act either from the Trust responding to a request for information or through making information accessible via the Trust's Freedom of Information Publication scheme on the SaTH website.

9.4 Information Security

Rules and guidance on information security are set out in the Information and Information Systems Security Policy available on the organisations' intranet.

9.4.1 Data Protection Impact Assessment (DPIA)

All new projects, processes, services and systems (including software and hardware) which are introduced must meet confidentiality and data protection requirements. To enable the Trust to address the privacy concerns and potential risks, a technique referred to as a Data Protection Impact Assessment (DPIA) must be used. A DPIA will assist to:

- Identify privacy risks to individuals.
- Protect the Trust's reputation.
- Ensure person identifiable data is being processed legally and securely.
- Identify potential problems and negotiate solutions.
- Identify all Information Assets and corresponding data flows.

Appendix 1 – Data Protection Impact Assessment template

9.4.2 Information Sharing

The Trust ensures that information sharing takes place within a structured and documented process in line with GDPR, Information Commissioner's Data Sharing Code of Practice and in accordance with the Health and Social Care Act 2012 and Health and Social Care (Safety and Quality) Act 2015.

A central record of Data Sharing Agreements (DSA) that the Trust have signed up to are available from the Information Governance Department.

Further information can be found within the Over-Arching Data Sharing Protocol which provides some guidance and a useful DSA template.

9.4.3 Information Assets

The tools to share data (personal or not) e.g. information system, hard copy, electronic, are considered Information Assets. IAs are identifiable and definable assets owned or contracted by an organisation which are 'valuable' to the business of that organisation. These IA should have Information Asset Owners who have the responsibility to ensure their IA is recorded in the Information Asset Register (IAR) together with details of their business criticality, data flow and any risk reviews carried out (via the Data Privacy Impact Assessment). The Information Asset may also have an Information Asset Administrator who administers the data on a day to day basis. All identified Trust IAs must be recorded in the IAR.

Further information on this can be found within the Information Asset Management Policy.

9.5 Sharing Confidential Information Without Consent

It may sometimes be necessary to share confidential information without consent or where the individual has explicitly refused consent. There must be a legal basis for doing so (e.g. to safeguard a child) or a court order must be in place. In deciding on any disclosure certain considerations and steps need to be taken:

- Discuss the request with the appropriate personnel such as the Caldicott Guardian and/or SIRO.
- Disclose only that information which is necessary or prescribed by law.
- Ensure the recipient is aware that they owe a duty of confidentiality to the data subject.
- Document and justify the decision to release the information
- Take advice in relation to any concerns you may have about risks of significant harm if the information is not disclosed.
- Follow any locally agreed information sharing protocols and national guidance.

Requests may be received by other agencies which are related to enforcement such as:

- The Police or another enforcement agency where the appropriate section 29 request form (in line with the Access to Records procedure) needs to be submitted from the law enforcement agency in order for the Trust to consider the request.
- The Local and National Counter Fraud specialists in relation to any actual or suspected fraudulent activity.

Health and Social Care professionals should have the confidence to share information in the best interests of their patients within the framework set out by these principles. They should be supported by the policies of their employees, regulators and professional bodies.

9.6 Confidentiality, Conversations and Social Media

Where during the course of your work you have conversations relating to confidential matters which may involve discussing or disclosing information about individuals such as staff members or patients, you must ensure:

- That the person you are sharing the information with has a legitimate relationship with the data subject
- Checks with individuals are made about contact preferences.
- Discussions such as this take place where they cannot be overheard.
- That, for telephone calls the rule is you do not give out confidential information over the phone – unless you are certain as to the identity of the caller and they have a legal basis to receive such information (e.g. you may need to speak to another team member on the phone who is based in another location).
- Where you receive a request over the telephone for confidential information ask the caller to put the request in writing so details can be verified.
- That you do not discuss confidential work matters in public places or at social occasions.
- Where an answer machine is used ensure that recorded conversations on the phone cannot be overheard or otherwise inappropriately accessed. Also, any 'confidential' information is kept to the minimum.

Do not share any personal information about patients, staff or anyone with an association with the Trust on social media.

9.7 Records Management

The Trust's Records Management policy and the Records Management NHS Code of Practice should be followed for all aspects of the record creation, storage, retention and destruction.

9.8 Access to Records and individual rights to their personal data

Individuals (data subjects) have a right to request access or copies of their records in line with the Data Protection Act by making a 'Subject Access Request' e.g. copies of 'personnel files'. Staff should familiarise themselves with the Trusts Subject Access Request procedures, also the Trust's 'Access to Health Records' procedure which should be followed for requests for data relating to their 'healthcare and treatment'.

Subject access requests must be completed within 30 days and provided free of charge (unless a request is "manifestly unfounded or excessive").

Unless subject to an exemption, individuals (patients and staff) have the following rights with respect to their personal data:

- The right to be informed - Individuals have the right to be informed about the collection and use of their personal data. This is a key transparency requirement under the GDPR. This can be done by using a privacy notice.
- The right of access – Individuals have the right to access their personal data. This is commonly referred to as subject access request.
- The right to rectification - The right to request that the Trust corrects any data if it is found to be inaccurate or out of date;
- The right to erasure - The right to request their personal data is erased where it is no longer necessary for the Trust to retain such information;
- The right to restrict processing - The right, where there is a dispute in relation to the accuracy or processing of their personal data, to request a restriction is placed on further processing;
- The right to data portability - The right to request that the Trust provides them with their personal information and where possible, to transmit that data directly to another data controller, where their information has been processed with their consent. Only applies to information provided by the data subject, where processed on a basis of consent or where necessary for performance of a contract; and carried out by automated means. The 'Data Portability' does not apply to the majority of 'paper' files.
- The right to object - The right to object to the processing of their data
- The right to withdraw their consent to the processing at any time if they have previously given consent for processing;
- Rights in relation to automated decision making and profiling - The GDPR applies to all automated individual decision-making and profiling. The Trust can only carry out this type of decision-making where the decision is:
 - necessary for the entry into or performance of a contract; or
 - authorised by Union or Member state law applicable to the controller; or
 - based on the individual's explicit consent.

Data subjects also have the right to lodge a complaint with the Information Commissioner's Office. For further information about individual's rights this can be found in the Information Commissioners Office at: <https://ico.org.uk/>

Further information relating to the accessing of records can be made found on the Trust external website.

10. Data Breaches

The Data Security and Protection Toolkit (DSPT) national measures are intended to help prevent confidentiality and security mistakes occurring. If they are sound and function well as preventative internal controls, they should help to eliminate mistakes. Retrospective Error Cause Removal is often the most time-consuming of all processes when dealing with complicated systems, so we should be aiming to "*do it right the first time*".

All staff need to know how to report data security incidents. All actual, potential or suspected data breaches, must be reported:

- on the Datix Incident reporting system by the person who has identified the breach of information or their line manager.
- notify your line-manager or IG Lead / Data Protection Officer as soon as possible, so they can assess how serious the incident is and start an investigation.

All incidents involving patient data are reported to the Caldicott Guardian.

The SIRO alongside the Data Protection Officer should consider whether serious breaches of confidentiality or those involving large numbers 'bulk data' of individuals need to be reported to the Information Commissioner and other regulatory bodies via the Data Security and Protection Toolkit (DSPT). The same process applies to Cyber Security Incidents. Serious incidents must be reported on SIRI within 72 hours of being identified so it is imperative that data breaches are reported as soon as possible.

Any breach of the data protection regulations or failure to adequately protect information / data held about patients, staff or the business of the Trust will be investigated by the IG Team and the direct line manager. Refer to the Disciplinary Policy W7 for further information on this.

10.1 What should be reported on Datix?

Misuses of personal data security incidents must be reported so that steps can be taken to rectify the problem and ensure that the same problem does not occur again. The following list provides some examples of breaches of this policy which should be reported:

- Sharing of passwords and/or Smartcards
- Unauthorised access to the Trust's computer systems either by staff or a third party
- Unauthorised access to personal confidential information where the member of staff does not have a need to know (legitimate relationship) e.g. sending an email to the wrong email recipient

- Disclosure of personal data to a third party where there is no justification and you have concerns that it is not in accordance with the data protection principles and the NHS Code of Confidentiality.
- Sending data in a way that breaches security and confidentiality e.g. non secure email addresses, no encryption of documents and fax machines.
- Leaving confidential information lying around and accessible in a public area, e.g. clinic areas or photocopiers.
- Theft, loss and potential loss of patient/staff identifiable information
- Disposal of confidential material in a way that breaches confidentiality, i.e. disposing of patient documentation, patient demographic labels in ordinary waste paper bins.
- Processing/transferring to others identifiable information without it being recorded as a dataflow and on the Information Asset Register (IAR). Refer to the Information Asset Policy.

Further information can be found within the standard operating procedure for the management of information governance serious incidents requiring investigations.

10.2 Assessing risk to the rights and freedoms of a data subject

The GDPR gives interpretation as to what might constitute a high risk to the rights and freedoms of an individual. This may be any breach which has the potential to cause one or more of the following:

- Loss of control of personal data
- Limitation of rights
- Discrimination
- Identity theft
- Fraud
- Financial loss
- Unauthorised reversal of pseudonymisation
- Damage to reputation
- Loss of confidentiality of personal data protected by professional secrecy
- Other significant economic or social disadvantage to individuals.

11. Contracts

- The GDPR makes written contracts between controllers and processors a general requirement, rather than just a way of demonstrating compliance with the seventh data protection principle (appropriate security measures) under the DPA.
- A contract (when PID is shared) alongside a data privacy impact assessment, should be used when dealing with an external provider during the procurement process.
- These contracts must now include certain specific terms, as a minimum.
- These terms are designed to ensure that processing carried out by a processor meets all the requirements of the GDPR (not just those related to keeping personal data secure).
- The GDPR envisages that adherence by a processor to an approved code of conduct or certification scheme may be used to help controllers demonstrate that they have chosen a suitable processor.

- The GDPR gives processors responsibilities and liabilities in their own right, and processors as well as controllers may now be liable to pay damages or be subject to fines or other penalties.

When is a contract needed?

Whenever a controller uses a processor (a third party who processes personal data on behalf of the controller) it needs to have a written contract in place. Similarly, if a processor employs another processor it needs to have a written contract in place.

Why are contracts between controllers and processors important?

Contracts 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 contracts by controllers and processors may also increase data subjects' confidence in the handling of their personal data

What needs to be included in the contract?

Contracts must set out the subject matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subject, and the obligations and rights of the controller.

Contracts must also include as a minimum the following terms, requiring the processor to:

- only act on the written instructions of the controller;
- ensure that people processing the data are subject to a duty of confidence;
- take appropriate measures to ensure the security of processing;
- only engage sub-processors with the prior consent of the controller and under a written contract;
- assist the controller in providing subject access and allowing data subjects to exercise their rights under the GDPR;
- assist the controller in meeting its GDPR obligations in relation to the security of processing, the notification of personal data breaches and data protection impact assessments;
- delete or return all personal data to the controller as requested at the end of the contract; and
- submit to audits and inspections, provide the controller with whatever information it needs to ensure that they are both meeting their Article 28 obligations, and tell the controller immediately if it is asked to do something infringing the GDPR or other data protection law of the EU or a member state.

All contracts (renewals / new services) must be shared with the Data Protection Officer.

12. Documentation

What's new under the GDPR?

- The documentation of processing activities is a new requirement under the GDPR.
- There are some similarities between documentation under the GDPR and the information the Trust provided to the ICO as part of registration under the Data Protection Act 1998.
- The Trust is required to have in place a record of our processing activities.

What is documentation?

- Most organisations are required to maintain a record of their processing activities, covering areas such as processing purposes, data sharing and retention; the ICO call this documentation.
- Documenting the processing activities is important, not only because it is itself a legal requirement, but also because it can support good data governance and help the Trust to demonstrate our compliance with other aspects of the GDPR.

A central record of processing activities is maintained by the Data Protection Officer, in the form of the Information Asset Register.

13. Data Protection by design and default

The GDPR introduces new obligations that requires the Trust to integrate data protection concerns into every aspect of its processing activities. This approach is 'data protection by design and by default'. These are key elements of the GDPR's risk-based approach and its focus on accountability, ie you are able to demonstrate how you are complying with its requirements. However, data protection by design and by default is not new. It is essentially the GDPR's version of 'privacy by design'.

The GDPR requires the Trust to put in place appropriate technical and organisational measures to implement the data protection principles and safeguard individual rights. This is 'data protection by design and by default'. In essence, this means we have to integrate or 'bake in' data protection into our processing activities and business practices, from the design stage right through the lifecycle.

Data protection by design is about considering data protection and privacy issues upfront in everything we do. It can help to ensure that we comply with the GDPR's fundamental principles and requirements, and forms part of the focus on accountability.

Within article 25 Data Protection Act, specifies that, as a controller, the Trust has responsibility for complying with data protection by design and by default

What is the Trust required to do?

The Trust must put in place appropriate technical and organisational measures designed to implement the data protection principles and safeguard individual rights.

The key is that we consider data protection issues from the start of any processing activity, and adopt appropriate policies and measures that meet the requirements of data protection by design and by default.

Some examples of how you can do this include:

- minimising the processing of personal data;
- pseudonymising personal data as soon as possible;
- ensuring transparency in respect of the functions and processing of personal data;
- enabling individuals to monitor the processing; and
- creating (and improving) security features.

Data Protection by design and default should be considered by all.

14. International Transfers

- The GDPR primarily applies to controllers and processors located in the European Economic Area (the EEA) with some exceptions.
- Individuals risk losing the protection of the GDPR if their personal data is transferred outside of the EEA.
- On that basis, the GDPR restricts transfers of personal data outside the EEA, or the protection of the GDPR, unless the rights of the individuals in respect of their personal data is protected in another way, or one of a limited number of exceptions applies.
- A transfer of personal data outside the protection of the GDPR (which we refer to as a 'restricted transfer'), most often involves a transfer from inside the EEA to a country outside the EEA.

By completing a Data privacy Impact Assessment alone or with a data processor/ controller can provide you with the information to understand whether there would be any risk of international transfer of data.

15. Exemptions

In some circumstances, the DPA 2018 provides an exemption from particular GDPR provisions. If an exemption applies, you may not have to comply with all the usual rights and obligations.

There are several different exemptions; these are detailed in Schedules 2-4 of the DPA 2018. They add to and complement a number of exceptions already built in to certain GDPR provisions.

The exemptions in the DPA 2018 can relieve you of some of your obligations for things such as:

- the right to be informed;
- the right of access;
- dealing with other individual rights;
- reporting personal data breaches; and
- complying with the principles.

Some exemptions apply to only one of the above, but others can exempt you from several things. Some things are not exemptions. This is simply because they are not covered by the GDPR. Here are some examples:

- Domestic purposes – personal data processed in the course of a purely personal or household activity, with no connection to a professional or commercial activity, is outside the GDPR’s scope. This means that if you only use personal data for such things as writing to friends and family or taking pictures for your own enjoyment, you are not subject to the GDPR.
- Law enforcement – the processing of personal data by competent authorities for law enforcement purposes is outside the GDPR’s scope (e.g. the Police investigating a crime). Instead, this type of processing is subject to the rules in Part 3 of the DPA 2018.
- National security – personal data processed for the purposes of safeguarding national security or defense is outside the GDPR’s scope. However, it is covered by Part 2, Chapter 3 of the DPA 2018 (the ‘applied GDPR’), which contains an exemption for national security and defense.

16. Implementation and Training

To comply with the law and with central NHS guidelines relating to Data Security and Protection (DSP), training is mandatory for all NHS staff (in the same way as health and safety training) the DSP toolkit mandates that:

A good level of DSP understanding enables all staff to understand more directly how such awareness, or lack of it, can impact on the organisation’s ability to function legally, effectively and ethically.

Improved awareness should result in better protection of confidential information from unauthorised staff, patients and visitors; inadvertent disclosure and theft, etc. Well protected records are less likely to fall into the wrong hands and are less likely to be compromised or misused. This is of particular significance in respect of personal information – i.e. personnel records or patient identifiable information. If staff, patients, suppliers, etc., perceive an NHS organisation to be reliable in handling their healthcare, information and business they will be more inclined to view that organisation as trustworthy.

All staff will be made aware of this revised policy via their line managers, induction or DSP training.

The Trust currently offers a variety of methods for annual data security and protection training and these can be found on the staff intranet.

17. Monitoring Compliance

Aspect of compliance or effectiveness being monitored	Monitoring method	Responsibility for monitoring	Frequency of Monitoring	Group or Committee that will review the findings and monitor completion of any resulting action plan
---	-------------------	-------------------------------	-------------------------	--

<p>Non-Compliance (IG breaches) will be highlighted via the Trust Datix system for Incident Reporting, which require investigation by the IG Team</p>	<p>Spot compliance checks to identify any high risk processes.</p> <p>Monitoring any datix trends and gaps in knowledge</p>	<p>The Information Asset Owner (IAO) / line management in respective data areas.</p> <p>DSP Toolkit Assertion Owners.</p> <p>IG Team</p>	<p>Regular compliance checks, every quarter, should be under-taken to provide assurance to the IAO/IG team.</p>	<p>Where non-compliance is reported these and the actions are reported to the IG Group. Where 'Serious Incidents' are identified, the SIRO / Caldicott Guardian will be notified and an investigation launched by the IG Manager / DPO.</p> <p>Any high IG risks will be reported to the Operational Risk Group.</p>
---	---	--	---	--

18. Equality Impact Assessment

This document has been subject to an Equality Impact Assessment. Please refer to the EQIA form.

19. Consultation process

This policy will be sent to the members of the Information Governance Group and any other key stakeholders before being sent to the Policy Approval Group.

20. Associated documents

- Information Governance & Framework Policy
- Information and Information Systems Security Policy
- Over-arching Data Sharing Protocol
- Reporting of security / confidentiality breaches/incidents
- Access to Health Records
- Subject Access Requests
- Information Asset Management policy
- Standard Operating Procedure for the Management of Information Governance Serious Incidents Requiring Investigation (SIRI)

21. Other Legislation and External References

Human Rights Act 1998

Article 8 of the Human Rights Act 1998 established a right to respect for private and family life, home and correspondence. This reinforces the duty to protect privacy of individuals and preserve the confidentiality of their health and social care records.

There should be no interference with the exercise of this right except as is in accordance with the law and is necessary in a democratic society in the interests of national security, public

safety, the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

Common Law Duty of Confidentiality

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:

- Where the individual to whom the information relates has consented
- Where disclosure is in the overriding public interest; OR
- Where there is a legal duty to do so, for example a court order

The common law applies to information of both living and deceased patients.

Caldicott Principles

Dame Fiona Caldicott produced a report in 1997 on the use of patient information which resulted in the establishment of Caldicott Guardians across the NHS Structure. She was asked to conduct a further review and a new report: 'Information to share or not to share' was published in March 2013. The recommendations of this report have been largely accepted by the government and a revised set of Caldicott Principles were published:

1. *Justify the purpose(s)* Every proposed use or transfer of personal confidential data within or from an organisation should be clearly defined, scrutinised and documented with continuing uses regularly reviewed, by an appropriate guardian.
2. Don't use personal confidential data unless it is absolutely necessary Personal Confidential data items should not be included unless it is essential for the specified purpose(s) of that flow. The need for patients to be identified should be considered at each stage of satisfying the purpose(s).
3. Use the minimum necessary personal confidential data Where use of personal confidential data is considered to be essential, the inclusion of each individual item of data should be considered and justified so that the minimum amount of personal confidential data is transferred or accessible as is necessary for a given function to be carried out.
4. Access to personal confidential data should be on a strict need-to-know basis Only those individuals who need access to personal confidential data should have access to it, and they should only have access to the data items that they need to see. This may mean introducing access controls or splitting data flows where one data flow is used for several purposes.
5. Everyone with access to personal confidential data should be aware of their responsibilities Action should be taken to ensure that those handling personal confidential data - both clinical and non-clinical staff - are made fully aware of their responsibilities and obligations to respect patient confidentiality.

6. Understand and comply with the law Every use of personal confidential data must be lawful. Someone in each organisation handling personal confidential data should be responsible for ensuring that the organisation complies with legal requirements.

7. *The duty to share information can be as important as the duty to protect patient confidentiality* Health and Social Care professionals should have the confidence to share information in the best interests of their patients within the frameworks set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies.

The Caldicott Guardian also has a strategic and operational role, which involves representing and championing confidentiality and information sharing requirements and issues at senior management level and, where appropriate, at a range of levels within the organisation's overall governance framework.

In 2014, the post of National Data Guardian (NDG) was established, with the role of helping to make sure the public can trust their confidential information is securely safeguarded and make sure that it is used to support citizens' care and to achieve better outcomes from health and care services. The NDG security standards underpin the new DSP Toolkit.

Information Commissioners Office Codes of Practice

The Trust processes data that is covered in the following Codes of Practice (2011) published by the Information Commissioner's Office (ICO):

- Data sharing
- Subject access
- Closed Circuit Television (CCTV)
- Privacy Notices
- Employment Practices
- Anonymisation
- Personal Information Online
- Privacy Impact Assessments

The codes of practices are due to be revised in line with the Data Protection Law 2018.

ICO GDPR Guidance at:

<https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf>

The Data Protection Act 2018 available at:

<https://www.gov.uk/government/collections/data-protection-act-2018>

NHS Digital (formerly Health and Social Care Information Centre) Guidance

This organisation was established in April 2013 and is responsible for facilitating the management and sharing of data across the NHS to support both operational and other functions such as planning, research and assessments.

Directions from NHS England allow NHS Digital to capture local healthcare information for commissioning purposes. To enable intelligent commissioning of healthcare services, NHS Digital collects, analyses, and processes healthcare data into a format that allows the appropriate commissioners access to the relevant data. In doing this, the Data Services for Commissioners programme allows commissioners access to the appropriate information without compromising patient confidentiality or statutory legal requirements surrounding the use of this data.

HSCIC (prior to NHS Digital) produced a Code of Practice: 'A Guide to Confidentiality in Health and Social Care' in September 2013:

1. Confidential information about service users or patients should be treated confidentially and respectfully.
2. Members of a care team should share confidential information when it is needed for the safe and effective care of individuals.
3. Information that is shared for the benefit of the community should be anonymised.
4. An individual's right to object to the sharing of confidential information about them should be respected.
5. Organisations should put policies, procedures and systems in place to ensure the confidentiality rules are followed

NHS X

Strategic information governance advice is now being provided by NHSX and guidance can be found on their website. This replaces the Information Governance Alliance (IGA). NHSX is leading the largest digital health and social care transformation programme in the world and this includes:

Coordination and consistency

- Setting national policy for NHS technology, digital and data (including data-sharing and transparency)
- Setting the strategy, developing best practice guidance, coordinating activities across the arms-length bodies and national or central programmes
- Becoming a single point of accountability for national digital transformation programmes and the oversight of NHS Digital

Setting standards

- Developing, agreeing and mandating clear standards (for example, on user experience, open standards, information governance, and open source) for the use of technology in the NHS
- Making sure that NHS systems become interoperable and that the NHS can incorporate the latest innovations without breaking the technical plumbing underneath

The NHS and Social Care Record Guarantees for England

The NHS and Social Care Record Guarantees for England sets out the rules that govern how individual care information is used in the NHS and in Social Care. It also sets out what control the individual can have over this.

Individuals' rights regarding the sharing of their personal information are supported by the Care Record Guarantees, which set out high-level commitments for protecting and safeguarding service user information, particularly with regard to: individuals' rights of access to their own information, how information will be shared (both within and outside of the organisation) and how decisions on sharing information will be made.

NHS Act 2006

Section 251 of the NHS Act 2006 allows the Common Law Duty of Confidentiality to be set aside by the Secretary of State for Health in specific circumstances where anonymised information is not sufficient and where patient consent is not practicable.

Health and Social Care Act 2012

The Health and Social Care Act 2012 provides NHS Digital with a legal basis to process identifiable data and on behalf of other NHS organisations. The Act provides the authority to operate Data Service for Commissioners (DSfC) and Data Service for Commissioners Regional Offices (DSCROs).

Health and Social Care (Safety and Quality) Act 2015

The Health and Social Care (Safety and Quality) Act 2015 sets the expectation that information will be shared between health and social care in the interests of individuals. Individuals are able to override such sharing if they have an objection. The Act is seen as key to enabling the Caldicott principle of there being a duty to share between those health and social care professionals involved in the direct care of patients if it is in the best interests of those individuals.

Computer Misuse Act 1990

This Act makes it illegal to access data or computer programs without authorisation and establishes three offences:

- Access data or programs held on computer without authorisation. For example, to view test results on a patient whose care you are not directly involved in or to obtain or view information about friends and relatives.
- Access data or programs held in a computer without authorisation with the intention of committing further offences, for example fraud or blackmail.
- Modify data or programs held on computer without authorisation

Appendix 1

Data Protection Impact Assessment (DPIA) Checklist for New or Existing Systems / Assets / Projects / changes in procedure

1. Introduction

The General Data Protection Regulation (GDPR) requires organisations to have appropriate technical and organisational measures in place to implement data protection principles and safeguard individual rights. This is “data protection by design and by default”.

The data protection principles should be built into our processing activities and business practices, from the design stage right through the lifecycle.

Under GDPR this is now a legal requirement.

Data protection by design is about considering data protection and privacy issues upfront in everything we do. It can help to ensure that we comply with the GDPR’s fundamental principles and requirements, and forms part of the focus on accountability.

Next Steps:

1. **Read this briefing note;**
2. **Start to complete the DPIA Template in Appendix 1 – fill out as much as possible;**
3. **Meet with the Data Protection Officer to discuss final assessment. Contact details are sath.informationgovernance@nhs.net**

2. Overview

- **A Data Protection Impact Assessment (DPIA) is a process to help you identify and minimise the data protection risks of a project.**
- **A DPIA must be completed for processing that is likely to result in a high risk to individuals. This includes some specified types of processing.**
- **It is also good practice to do a DPIA for any other major project which requires the processing of personal data.**

In general the DPIA must include the following:

- **describe the nature, scope, context and purposes of the processing;**
- **assess necessity, proportionality and compliance measures;**
- **identify and assess risks to individuals**
- **identify any additional measures to mitigate those risks.**

To assess the level of risk, you must consider both the likelihood and the severity of any impact on individuals. High risk could result from either a high probability of some harm, or a lower possibility of serious harm.

If you identify a high risk that you cannot mitigate, you must consult with Data Protection Officer before starting the processing.

3. What is a Data Privacy Impact Assessment (DPIA)?

There is a requirement under the General Data Protection Regulation (GDPR) to put in place appropriate technical and organisational measures to implement the data protection principles and safeguard individual rights. This is 'data protection by design and by default'. This is a key element of the accountability requirements in the legislation.

Under the General Data Protection Regulation (GDPR) we have an obligation to conduct a Data Protection Privacy Impact Assessment (DPIA) before carrying out types of processing likely to result in high risk to individuals' interests. If the DPIA identifies a high risk that cannot be mitigated please consult the Data Protection Officer.

A DPIA is a way for you to systematically and comprehensively analyse your processing and help you identify and minimise data protection risks.

DPIAs should consider compliance risks, but also broader risks to the rights and freedoms of individuals, including the potential for any significant social or economic disadvantage. The focus is on the potential for harm - to individuals or to society at large, whether it is physical, material or non-material.

To assess the level of risk, a DPIA must consider both the likelihood and the severity of any impact on individuals.

A DPIA does not have to eradicate the risks altogether, but should help to minimise risks and assess whether or not remaining risks are justified.

DPIAs are a legal requirement for processing that is likely to be high risk. But an effective DPIA can also bring broader compliance, financial and reputational benefits, helping you demonstrate accountability and building trust and engagement with individuals.

A DPIA may cover a single processing operation or a group of similar processing operations. A group of controllers can do a joint DPIA.

It's important to embed DPIAs into your organisational processes and ensure the outcome can influence your plans. A DPIA is not a one-off exercise and you should see it as an ongoing process, and regularly review it

4. When is a DPIA needed?

A DPIA must be completed before you begin any type of processing which is "likely to result in a high risk". This means that although you have not yet assessed the actual level of risk you need to screen for factors that point to the potential for a widespread or serious impact on individuals.

In particular GDPR says you must do a DPIA if you plan to:

- **use systematic and extensive profiling with significant effects;**
- **process special category or criminal offence data on a large scale; or**
- **Systematically monitor publicly accessible places on a large scale.**

And the Information Commissioner's Office (ICO) also requires the Trust to do a DPIA if we plan to:

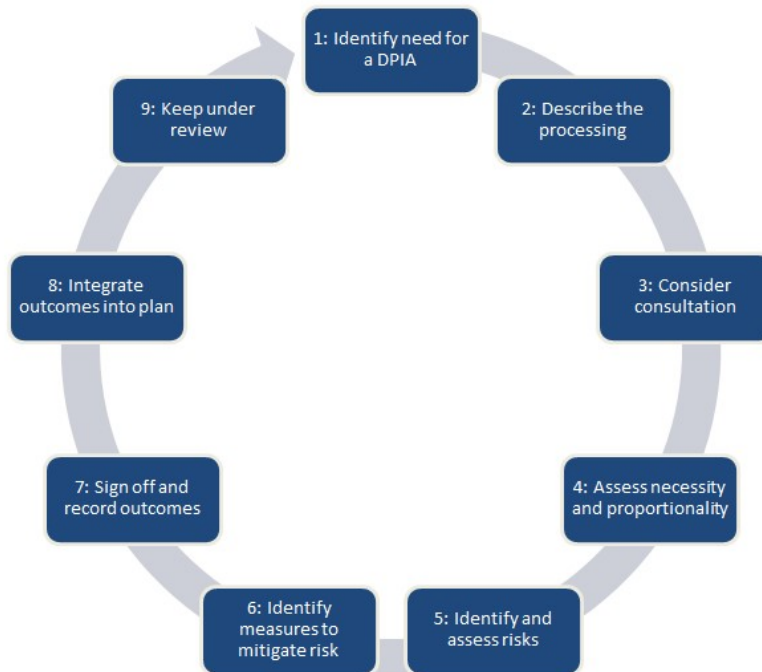
- **use new technologies;**
- **use profiling or special category data to decide on access to services;**
- **profile individuals on a large scale;**
- **process biometric data;**
- **process genetic data;**
- **match data or combine datasets from different sources;**
- **collect personal data from a source other than the individual without providing them with a privacy notice ('invisible processing');**
- **track individuals location or behaviour;**
- **profile children or target marketing or online services at them; or**
- **process data that might endanger the individual's physical health or safety in the event of a security breach.**

Other examples of when a DPIA is needed are:

- **that is large scale processing;**
- **involves profiling or monitoring,**
- **decides on access to services or opportunities;**
- **or involves sensitive data of vulnerable individuals.**

Even if there is no specific indication of likely high risk, it is good practice to do a DPIA for any major new project involving the use of personal data.

A DPIA should begin early in the life of a project, before processing commences, and run alongside the planning and development process. It should include these steps:



You must seek the advice of your Data Protection Officer and also consult with individuals and other stakeholders throughout this process.

When the DPIA identifies a high risk and measures cannot be taken to reduce that risk the processing of information cannot commence until the Data Protection Officer has been consulted and given advice. This may also include seeking advice from the Information Commissioner's Office (ICO) and gaining the approval from the Senior Information Risk Officer (SIRO).

Once the DPIA has been completed, the risks assessed and the document signed, it should be saved as part of the project paperwork and presented by the Project Lead to the relevant Project Team and then the Project Board, or appropriate governance process, for a formal decision regarding how to proceed with the project.

Appendix 1

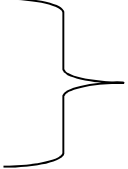

Please complete all questions with as much detail as possible.

Project Lead:		Contact Details:	
Information Asset Owner (who will be responsible for the system once project completed)		Contact Details:	
Changes in procedure, identify a named person for this change		Contact Details:	
Date:			

Project Title and Description: (summary of project, why it is required and the identify the need for this DPIA)	
Cross reference to other projects:	
Relationships: (e.g. other organisations involved)	
Stakeholders identified:	

DPIA key questions

Question	Response
<p>1.a Will the new system or application contain personal identifiable data or sensitive data?</p> <p>If answered 'No' you do not need to complete any further questions as a DPIA is not required.</p>	<p><input type="checkbox"/> Yes</p> <p><input type="checkbox"/> No</p> <p>If yes it will involve data for:</p> <p><input type="checkbox"/> Patient</p> <p><input type="checkbox"/> Staff</p> <p><input type="checkbox"/> Other (please specify)</p>
<p>1.b Will the new system process any transactions such as those described within the Payment Card industry (PCI) as described on the ICO website- https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/security/</p>	<p><input type="checkbox"/> Yes</p> <p><input type="checkbox"/> No</p> <p>If yes, please describe how the supplier / system/ trust will meet the PCI data security standards below:</p>
<p>2. Please state the purpose for the collection of the data e.g. patient treatment, research, audit etc.</p> <p>What safeguards are there to prevent "function creep" i.e. the information being used for additional extended purposes</p>	
<p>3. What is your lawful basis for processing?</p> <p>If you need any further guidance on the legal basis please contact the Data Protection Officer</p>	<p><input type="checkbox"/> Consent (GDPR Article 6 a)</p> <p><input type="checkbox"/> Contract ((GDPR Article 6b)</p> <p><input type="checkbox"/> Legal obligation (GDPR Article 6c)</p> <p><input type="checkbox"/> Vital interests (GDPR Article 6d)</p> <p><input type="checkbox"/> Public task (GDPR Article 6e)</p> <p><input type="checkbox"/> Legitimate interests (GDPR Article 6f)</p> <p><input type="checkbox"/> Special category data (GDPR Article 9h)</p>

<p>4. What is the nature of the data, and does it include special category or criminal offence data? Please tick the data items that are held in the system?</p> <p>Personal </p> <p>Special categories </p>	<ul style="list-style-type: none"> <input type="checkbox"/> Name <input type="checkbox"/> Address <input type="checkbox"/> Post Code <input type="checkbox"/> Date of Birth <input type="checkbox"/> Sex <input type="checkbox"/> GP <input type="checkbox"/> Consultant <input type="checkbox"/> NHS Number <input type="checkbox"/> Next of Kin <input type="checkbox"/> NI Number <input type="checkbox"/> Hospital No. <input type="checkbox"/> Photographs, digital images. <input type="checkbox"/> Passport number <input type="checkbox"/> Online identifiers and location data <input type="checkbox"/> Telephone Number <input type="checkbox"/> Criminal conviction and offences <input type="checkbox"/> Treatment dates <input type="checkbox"/> Medical/ Mental health & Diagnosis <input type="checkbox"/> Occupation <input type="checkbox"/> Sex life or sexual orientation <input type="checkbox"/> Religion or philosophical beliefs <input type="checkbox"/> Ethnic Origin <input type="checkbox"/> Political opinion <input type="checkbox"/> Trade union membership <input type="checkbox"/> Genetic / Biometric data Other please state here:
<p>5. If you are relying on Consent (6a) as your lawful basis, please state how you have gained explicit consent i.e. what are your methods, how is this recorded, do you have the ability to record when a patient withdraws their consent etc.</p> <p>Have patients/staff been informed of and given their consent to all the processing and disclosures?</p> <p>If yes, state how they have been informed? e.g. leaflet, poster, website etc. and provide a copy.</p>	<ul style="list-style-type: none"> <input type="checkbox"/> Yes <input type="checkbox"/> No
<p>6. Will the project /system collect new personal or sensitive data items which have not been collected by the Trust before?</p>	<ul style="list-style-type: none"> <input type="checkbox"/> Yes <input type="checkbox"/> No <p>If yes, what is the new personal/sensitive data?</p>

<p>If yes, we will need to alert the data subject with a privacy notice on website.</p>	
<p>7. Will the information be shared with any other organisations?</p>	<p><input type="checkbox"/> Yes</p> <p><input type="checkbox"/> No</p> <p>If yes confirm that there is a Data Sharing Agreement in place or other appropriate protocols/measures to mitigate risks and ensure adequate level of security</p>
<p>8. Describe the nature of the processing.</p> <p>i.e. How will you collect, use, store and delete data? What is the source of the data? Will it be stored via the cloud? If so how secure is this?</p> <p>You may find it useful to refer to a flow diagram or other way of describing data flows.</p>	
<p>10. How many individuals will be affected?</p> <p>Will it involve children/vulnerable groups?</p>	<p>Number of individuals affected:</p> <p><input type="checkbox"/> Yes</p> <p><input type="checkbox"/> No</p>
<p>11. Would they expect you to use their data in this way?</p>	<p><input type="checkbox"/> Yes</p> <p><input type="checkbox"/> No</p>
<p>12. Have there been any prior concerns over this type of processing or security flows?</p>	<p><input type="checkbox"/> Yes</p> <p><input type="checkbox"/> No</p>
<p>13. Do you plan to consult IT security experts, or any other experts?</p>	<p><input type="checkbox"/> Yes</p> <p><input type="checkbox"/> No</p>
<p>14. If applicable has the third party contract / supplier of the system registered with the Information Commissioner?</p> <p>What is their notification number?</p>	<p><input type="checkbox"/> Yes</p> <p><input type="checkbox"/> No</p> <p><input type="checkbox"/> N/A</p> <p>ICO Registration number:</p>
<p>15. Has a check been done on the supplier/third party been checked for any</p>	<p><input type="checkbox"/> Yes</p> <p><input type="checkbox"/> No</p>

enforcements or decision notices relating to data breaches?	
16. Does the third party / supplier, contract contain all the necessary Information Governance/ security clauses?	<input type="checkbox"/> Yes <input type="checkbox"/> No
17. Has the supplier / third party successfully completed a Data Security Protection toolkit or has the Trust assured itself separately that they reach a similar or higher data security standard.	<input type="checkbox"/> Yes <input type="checkbox"/> No
18. Has the method of transporting the information to, from and within the Trust changed? If yes, please state how the information will now be transported? e.g. email, phone, fax etc.	<input type="checkbox"/> Yes <input type="checkbox"/> No
19. If applicable, does the transfer of this information comply with the Trust's Information Governance Policy, Data Protection Policy and Information and Information Systems Security Policy?	<input type="checkbox"/> Yes <input type="checkbox"/> No
20. Will the information be kept up to date and the personal data checked for accuracy?	<input type="checkbox"/> Yes <input type="checkbox"/> No If yes, how often?
21. Is there a useable audit trail in place for the system if applicable? For example to identify who has accessed a record?	<input type="checkbox"/> Yes <input type="checkbox"/> No
21. Give details of how the information will be held/levels of access and please include whether the system / supplier has implemented any transactional monitoring techniques?	
22. What are the retention periods for this data and have they been documented?	
23. How will the data be destroyed after it is no longer necessary?	
24. Are you transferring any data outside the UK e.g. location of servers, data portability for data subject?	<input type="checkbox"/> Yes <input type="checkbox"/> No If yes, where?
25. Have any information risks been identified and if so, have these been assessed?	<input type="checkbox"/> Yes <input type="checkbox"/> No

For example – mobile devices – where will they be located? What information will be displayed?

Will this be in a public area? If so can the information being displayed be anonymised?

Would the system be susceptible to fraudulent activity e.g. identity theft,

Either answer, please complete the risk assessment form in-line with Trust Risk Management policy.

Sign off and record of outcomes

Item	Name/date	Notes
Measures approved by:	<i>IAO/Project lead electronic signature to be added with date</i>	Integrate actions back into project plan and risk register with date and responsibility for completion
Residual risks approved by:	<i>SIRO signature to be added with date</i>	If accepting any residual high risk, consult the ICO before going ahead
DPO advice provided:	<i>DPO signature to be added with date</i>	DPO should advise on compliance, measures and whether processing can proceed
Summary of DPO advice:		
DPO advice accepted or overruled by:		If overruled, you must explain your reasons
Comments:		
Consultation responses reviewed by:	<i>DPO signature to be added with date</i>	If your decision departs from individuals' views, you must explain your reasons
Comments:		
This DPIA will kept under review by:	<i>IAO/Project lead electronic signature to be added with date</i>	The DPO should also review ongoing compliance with DPIA