Privacy Impact Assessment

Redmoor Health

Reference No:	IG07
Version:	1.0
Purpose of Document:	Sets out the process for completing Privacy Impact Assessments to identify any impact on privacy where a new service or system is introduced
Ratified by:	Information Governance and Records Management Steering Group
Date ratified:	
Review Date	
Name of originator/ author:	
Contact details of originator/author	
Version:	Version 1.0
Distributed via:	Intranet

Version Record			
Version	Date	Status	Comment

Contents

A Privacy Impact Assessment (PIA) is a process which helps assess privacy risks to individuals in the collection, use and disclosure of personal information.

A failure to properly embed appropriate privacy protection measures may result in a breach of privacy laws, a declaration of incompatibility with the Human Rights Act, or prohibitive costs in retro-fitting a system to ensure legal compliance or address community concerns about privacy.

This template is a practical tool to help identify and address the data protection and privacy concerns at the design and development stage of a project, building data protection compliance in from the outset rather than bolting it on as an afterthought. This document details the process for conducting a Privacy Impact Assessment (PIA) through a project life-cycle to ensure that, where necessary, personal and sensitive information requirements are complied with and risks are identified and mitigated.

A PIA should be carried out whenever there is a change that is likely to involve a new use or significantly change the way in which personal data is handled, for example a redesign of an existing process or service, or a new process or information asset being is introduced.

Completion of a PIA should be built into the organisational business approval and procurement processes.

This procedure is to be considered in the following circumstances:

- introduction of a new paper or electronic information system to collect and hold personal data;
- update or revision of a key system that might alter the way in which the organisation uses, monitors and reports personal information.
- changes to an existing system where additional personal data will be collected
- proposal to collect personal data from a new source or for a new activity
- plans to outsource business processes involving storing and processing personal data
- plans to transfer services from one provider to another that include the transfer of information assets
- any change to or introduction of new data sharing agreements

This list is not exhaustive.

Any systems which do not identify individuals in any way do not require a PIA to be performed. However, it is important to understand that what may appear to be "anonymised" data, could in fact be identifiable when used with other information, so anonymised data should be considered very carefully before any decision is made that it will not identify individuals.

The Information Governance team will advise any services regarding whether a PIA needs to be completed and support them with review of the PIA template.

There is no statutory requirement for any organisation to complete a PIA. However, central

Government departments have been instructed to complete PIAs by Cabinet Office and the Department of Health has included PIAs as a standard in the Information Governance Toolkit . This template is based on the Information Commissioners Office guidance on implementation and use of PIAs and has been adapted for use within health settings.

Because organisations vary greatly in size, the extent to which their activities intrude on privacy, and their experience in dealing with privacy issues makes it difficult to write a 'one size fits all' guide. It is important to note now that not all of the information provided in this guide will be relevant to every project assessed and further discussion may be required by the Information Governance Lead.

The ICO recommends that projects which are already up and running are not submitted to a PIA process, but to either a compliance check or a data protection audit, whichever is more appropriate is completed. A full PIA includes a report and would be done in consultation with the IG lead if there were major issues identified though an initial PIA.

2. Who is responsible for completing a PIA?

Any person who is responsible for introducing new or revised service or changes a new system, process or information asset is (the Information Asset Owner – IAO) responsible for ensuring the completion of a PIA and therefore must be effectively informed of these procedures.

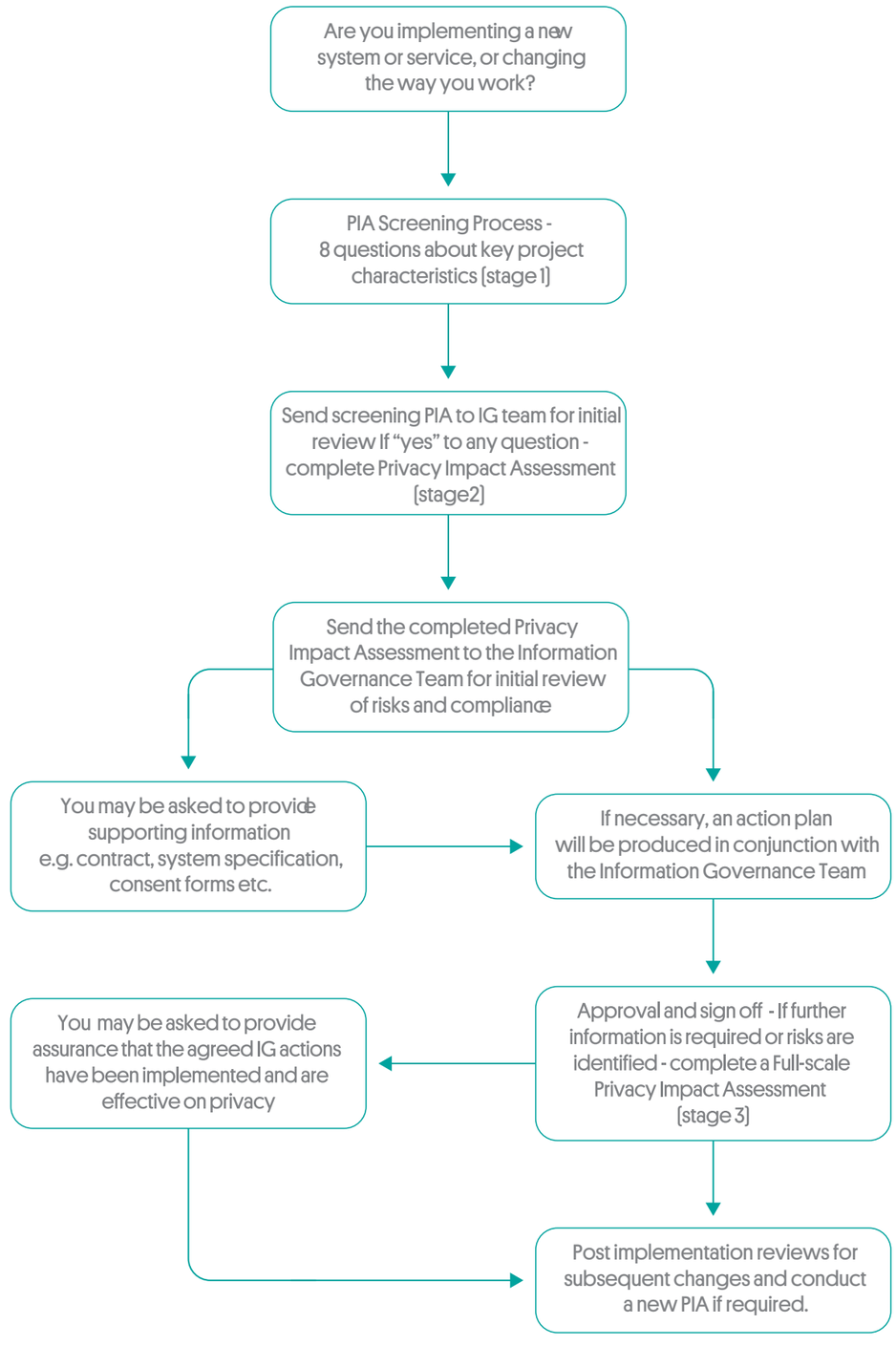
The Information Governance Lead should be consulted at the start of the design phase of any new service, process, purchase of implementation of an information asset etc. so that they can advise on the need and procedures for completing the PIA.

Privacy Impact Assessment outcomes should be routinely reported back to the organisation and issues raised through the project/programme board. Significant issue should be raised with the CG/SIRO in order for a risk assessment to be performed.

Regular CSU service reports will briefly report on PIAs reviewed and any significant issues identified.

Privacy Impact Assessment Flowchart

1. An Information Asset Operating systems, infrastructure, business applications, off-the-shelf products, services, user developed applications.



Three Stages of a PIA

Stage 1 - The initial screening questions

This section is to be completed by the service manager or project lead responsible for delivering the proposed change.

The purpose of the screening questions is to ensure that a further PIA assessment is required and ensure that the investment in the organisation is proportionate to the risks involved.

If response to any of the questions is “yes” then an initial Privacy Impact Assessment should be considered.

A meeting with the Information Governance lead should be arranged to review the responses and discuss whether a stage 2 assessment should be completed.

Stage 2 – Privacy Impact Assessment

The responses to the screening questions will give an indication as to the appropriate scale of the PIA. In some cases, the answers to the screening questions may not be known and the process will need to be re-visited when more information comes to light.

To be completed by the service manager or project lead responsible for delivering the proposed change (IAO). The completed form will be assessed by the Information Governance Lead who will advise on the next stage. There are three possible outcomes:

1. The PIA is incomplete and will have to be repeated or further information obtained.
2. The screening process has not identified any PIA concerns and the process is complete
3. The screening process has identified a low privacy impact and the associated risks require remedial action to address. An initial PIA is recommended.

This section includes an explanation of the data flows – the collection use and deletion of personal data should be described.

Compliance Checklist

The Privacy Impact Assessment also contains data mapping template and data protection and privacy law compliance checks which need to be considered by the IG lead. The checklist reviews the Data Protection Principles in order for each to be considered and should be completed by the PIA reviewer.

Stage 3 - Full-scale Privacy Impact Assessment

Where the initial PIA identifies further IG issues, an action plan should be developed on how the risks will be mitigated. This will include identified issues, associated actions, related roles and responsibilities and timescales and will be given to the Information Governance Lead for discussion within relevant Information Governance/other groups who will be responsible for the provision of expert advice and for ensuring that the remedial actions are implemented within agreed timescales.

The organisations Caldicott Guardian and/or Senior Information Risk Owner (SIRO) should be included at an early stage to ensure adequate consultation of the PIA.

Privacy Impact Assessment

This Privacy Impact Assessment must be completed wherever there is a change to an existing process or service, or a new process or information asset is introduced that is likely to involve a new use or significantly changes the way in which personal data is handled.

PIA Reference Number:	
Project Description:	Pilot the use of Skype to connect clinicians based in GP Practices to nursing homes
Implementing Organisation:	
Project Manager details: Name Designation Contact details	
Overview: [Summary of the proposal] What the project aims to achieve	Use of Skype to carry out a virtual clinic with nursing homes The aim of this project is to improve the connectivity between practices and nursing homes and reduce the number of unnecessary face to face contacts for consultations that could be undertaken remotely.
State the purpose of the project – eg patient treatment, administration, audit, research etc.	Patient assessment by clinician
Key stakeholders [including contact details]	
Implementation Date:	

Stage 1 – Initial Screening Questions

2. Guidance on what is classified as an Information Asset can be found at Note 1
3. Guidance on what is classed as personal data can be found at Note 2

Answering "Yes" to any of the screening questions below represents a potential IG risk factor that will have to be further analysed to ensure those risks are identified, assessed and fully mitigated.

Q	Category	Screening question	Yes/No
1.1	Identity	Will the project involve the collection of new information about individuals?	No
1.2	Identity	Will the project compel individuals to provide information about themselves?	Yes
1.3	Multiple organisations	Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?	No
1.4	Data	Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?	No
1.5	Data	Does the project involve using new technology which might be perceived as being privacy intruding for example biometrics or facial recognition?	Yes
1.6	Data	Will the project result in you making decisions or taking action against individuals in ways which could have a significant impact on them?	Yes
1.7	Data	Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example health records, criminal records, or other information that people are likely to consider as private?	Yes
1.8	Data	Will the project require you to contact individuals in ways which they may find intrusive?	Yes

If you have answered "Yes" to any of the questions below please proceed and complete stage 2

Stage 2 – Privacy Impact Assessment

4. Sensitive personal data as defined by section 2 of the Data Protection Act 1998 Additional statutory requirements apply

2.1	Is this a new or changed use of personal information that is already collected? See note 3 for guidance	It is a changed method of communicating with a patient.
2.2	What data will be collected? None, there will be no recording. The patient's condition will be discussed and summarised in GP electronic clinical system as per a normal face to face consultation.	
	Administration data Forename: Surname: DoB: Age: Gender: Address: Postcode: NHS No: Another unique identifier (please specify) : Other data (Please state): Sensitive data Racial or ethnic origin Political opinion Religious belief Trade Union membership Physical or mental health or condition Sexual life Commission or alleged commissionw of an offence Proceedings for any offence committed or alleged Will the dataset include clinical data? No Will the dataset include financial data No Description of other data collected: None Is the information being used for a different purpose than it was originally collected for? No	
2.3	Are other Organisations involved in processing the data?	No

	Name and Notification number	Data Controller (DC) or Data Processor (DP)?	Completed and compliant with the IG Toolkit	

2.4.	Has a data flow mapping exercise been undertaken? If yes, please provide a copy- template attached, if no, please undertake – see Note 4 and page 13 for guidance	No	
2.5	Does the Work involve employing contractors external to the Organisation? If yes, provide a copy of the confidentiality agreement or contract?	Yes	
2.6	Describe in as much detail why this information is being collected/used ? No information is being collected.		
2.7	Will the information be collected electronically, on paper or both?	Neither, it is a different type of communication with the patient, rather than data collection.	
2.8	Where will the information will be stored : No storage of information		
2.9	Will this information being shared outside the organisations listed above in question 3? If yes, describe who and why:	No	
2.10	Is there an ability to audit access to the information?	No information to access	
2.11	Does the system involve new links with personal data held in other systems or have existing links been significantly changed? No		
2.12	How will the information be kept up to date and checked for accuracy and completeness (data quality)? Not applicable		
2.13	Who will have access to the information? Not applicable		
2.14	What security and audit measures have been implemented to secure access to and limit use of personal identifiable information? To gain access to Skype accounts, the authentication process will be via a user name and password.		
2.15	Will any information be sent offsite – ie outside of the organisation and its computer network Are you transferring personal data to a country or territory outside of the EEA?	No	

5. The Information Governance Toolkit is a self-assessment tool provided by Connecting For Health to assess compliance to the Information Governance
6. For example Direct Patient Care, Statistical, Financial, Public Health Analysis, Evaluation. See NHS Confidentiality Code of Practice Annex C for examples of use.
7. Examples of Storage include bespoke system (eg SystmOne, SharePoint), Spreadsheet or database in Network Drive, server location, filing cabinet (office and location), storage area/filing room (and location) etc.

2.16	Please state by which method the information will be transferred? Email: (not NHS.net) × Fax × Nhs.net email × Courier × Website access × Post (internal) × Post (external) × By Hand × Telephone × Wireless network × Other (please specify)		
2.17	Are disaster recovery and contingency plans in place?	If there is no access to Skype, alternative arrangements will be made if the patient needs to see the GP	
2.18	Is Mandatory Staff Training in place for the following?: • Data Collection: • Use of the System or Service: • Collecting Consent: • Information Governance:	N/A Yes Yes Yes Also covered in the attached Standard Operating Procedure	Dates To be arranged with practice staff once go live date is agreed
2.19	Are there any new or additional reporting requirements for this project?	No	
	• Who will be able to run reports? • Who will receive the report or where will it be published? • Will the reports be in person-identifiable, pseudonymised or anonymised format?		
2.20	If this new/revised function should stop, are there plans in place for how the information will be retained / archived/ transferred or disposed of?	N/A	
2.21	How will individuals be informed about the proposed uses of their personal data?		
	Consent form (attached) Patient leaflet (attached)		
2.22	Are arrangements in place for recognising and responding to patients requests for access to their personal data?	N/A	
2.23	Will patients be asked for consent for their information to be collected and/or shared?	N/A	
	If no, list the reason for not gaining consent e.g. relying on an existing agreement, consent is implied, the project has s251 approval or other : How will you manage patient/service user dissent?		

Attachments include (see Note 5 for examples): Consent Form, Patient Leaflet, Standing Operating Procedure

3.0 Data Mapping

Stage 1 - The initial screening questions

Please complete the following data mapping exercise:

This data mapping should be completed pictorially using a box for each 'point of rest' of data, these numbered 1, 2 etc. The first seven of the below points should be answered in each box and then a connecting line between the boxes answering the last question about how data is moved. Where data is coming from various sources it will probably be easiest to have a box for each numbered 1a, 1b, 1c etc. and a line from each to box to 'point of rest' 2, as they may have different transport methods.

'Data at rest' includes electronic information in a system, spreadsheet or database or on paper in a filing system etc.

For each point of 'data at rest' the following points need to be considered:

1. What data fields are included e.g. first name, last name, date of birth, postcode, diagnosis etc?
   Please Enter in to the Data Fields Table (3.1)

2. How has the data been gathered? Eg Extract from existing system, questionnaire, consolidation etc.
   Please Enter in to the Data Fields Table (3.1)

3. Who has access to the data and what is the process for gaining access?

Please Enter in to the Data Mapping (3.2)

4. Is there an audit trail showing each time the data is accessed and by who?

Please Enter in to the Data Mapping (3.2)

5. What is the format of the data at this point and how is it stored? Eg paper, electronic, safe haven, encryption, security etc

Please Enter in to the Data Mapping (3.2)

6. Who is responsible for the data at this point?

Please Enter in to the Data Mapping (3.2)

7. Is the data to be shared? If so with whom? Eg will it be shared with other organisations such as PCT, GP practice, social services, community health, mental health etc

Please Enter in to the Data Mapping (3.2)

8. Please indicate how data is moved between the points of rest i.e. if electronically is it over a secure route such as local area network, NHSmail to NHSmail etc.

Please Enter in to the Data Mapping (3.2)

3.1 Data Fields Table

Box no (Data flow mapping exercise)	Name of Field	What is the source of the data? Which system is it from?	What is the source of the data? Which system is it from?

3.2 Data Mapping

Location	Transfer		Location
	what format is it? i.e. a spread sheet?		
3. 4. 5. 6. 7.		Sent: How is it sent? i.e. NHS mail Received: How is it received? i.e. NHS mail.	3. 4. 5. 6. 7.

Privacy Impact Assessment – Assessment of Legal Compliance

[to be completed by the IG lead]

PIA Reference No

Does the PIA meet the following legal requirements?

Data Protection Act

Principle	
Principle 1 – [2.21 2.23] Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless – (a) at least one of the conditions in Schedule 2 is met, and (b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met (See guidance sheet for more detailed explanation)	Patient is asked for consent at the point of contact. The process is explained to them and they have the opportunity to dissent.
Principle 2 – [2.2] Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.	Consultation is for medical purposes and patient has consented to take part.
Principle 3 – [3.1] Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.	Data is not retained after the consultation has concluded.
Principle 4 – [] 2.12 Personal data shall be accurate and, where necessary, kept up to date.	The consultation is summarised onto the medical records. Health care professionals should ensure that this is done as soon as possible if not contemporaneously
Principle 5 – [2.20] Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.	Data is not retained after consultation
Principle 6 – [2.22& 2.23] Personal data shall be processed in accordance with the rights of data subjects under this Act.	Patient has consented to take part in the process.
Principle 7 – [2.13 2.14 2.16 2.17 2.18] Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.	Equipment is secure and complies with the NHS standard for encryption
Principle 8 – [2.15] Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.	Not applicable

Common Law Duty of Confidentiality

	Assessment of Compliance
Has the individual to whom the information relates given consent?	YES
Is the disclosure in the overriding public interest?	Not applicable
Is the disclosure in the overriding public interest?	Not applicable
Is there a statutory basis that permits disclosure such as approval under Section 251 of the NHS Act 2006	Not applicable

Human Rights Act 1998

The Human Rights Act establishes the right to respect for private and family life. Current understanding is that compliance with the Data Protection Act and the common law of confidentiality should satisfy Human Rights requirements.

Will your actions interfere with the right to privacy under Article 8? – have you identified the social need and aims of the project? Are your actions a proportionate response to the social need?
Not applicable

Supporting Guidance for Completion of the Privacy Impact Assessment

1	Information Asset E.g. Operating systems, infrastructure, business applications, off-the-shelf products, services, user-developed applications, devices/equipment, records and information (extensive list).
2	Person Identifiable Data Key identifiable information includes: • patient's name, address, full post code, date of birth; • pictures, photographs, videos, audio-tapes or other images of patients; • NHS number and local patient identifiable codes; • anything else that may be used to identify a patient directly or indirectly. For example, rare diseases, drug treatments or statistical analyses which have very small numbers within a small population may allow individuals to be identified.
3	New use of information could include: - consistent with PIA Introduction The Commissioning of a new service Data Extracts involving new fields of patient confidential data Setting up a database or independent Patient System Reports Examples of changes to use of information could include: Moving paper files to electronic systems Collecting more data than before Using Data Extracts for a different purpose Additional organisations involved in information process Revisions to systems, databases (including mergers)
4	Data Flow Mapping A Data Flow Map is a graphical representation of the data flow. This should include: • Incoming and outgoing data • Organisations and/or people sending/receiving information • Storage for the 'Data at Rest' i.e. system, filing cabinet • Methods of transfer
5	Examples of additional documentation which may be required (copies): • Contracts • Confidentiality Agreements • Project Specification • System Specifications (including Access Controls) • Local Access Controls Applications • Information provided to patients • Consent forms

Privacy Impact Assessment - stage 3

Producing a PIA report

In most small scale projects the PIA may identify one or more IG risks and the lead manager will be advised on the actions necessary to mitigate or eliminate those risks.

Where the PIA discovers complex or several IG risks, the IG Lead will conduct a further more detailed assessment (a full scale PIA) and produce a report.

The final report should cover (where applicable):

- A description of the proposal including the data flow process
- The case justifying the need to process an individual's personal data and why the particular policy or project is important
- An analysis of the data protection issues arising from the project
- Details of the parties involved
- Details of the issues and concerns raised
- Discussions of any alternatives considered to meet those concerns, the consultation process, and the rationale for the decisions made
- A description of the privacy by design features adopted
- An analysis of the public interest of the scheme
- Compliance with the data protection principles
- Compliance with the Government Data Handling review's information security recommendations
- Where the proposal involves the transfer and storage of personal data the PIA should include details of any security measures that will be put into place to ensure the data is protected and kept secure.

Sign off Forms and agreed actions

Identified Risks, Agreed Actions and Sign Off Form.

What are the key privacy issues and associated compliance and corporate risks? (Some Privacy Issues may have more than one type of risk i.e. it may be a risk to individuals and a corporate risk)

Privacy Issue	Risk to Individuals	Compliance Risk	Corporate Risk

Describe the actions you could take to reduce the risk and any future steps which would be necessary (e.g. new guidance)

Risk	Solution (s)	Result: Is the risk reduced, eliminated or accepted?
Access to Personal data by persons other than the data subject. What records and logs are created by using the software?	Consultation is not recorded	Eliminated
The integrity of the computers used (how at risk are they from trojans or viruses)	Use of NHS equipment at both sites that complies with Dh standards of encryption	Reduced
Is suitable training available for the operators to ensure that they know what options the program is capable of and which of these are permitted to be used	Standard operating procedure has been developed for users of the system	Reduced
The medical professional would need to ensure that there was no third party data visible on desks or screens that could be viewed or captured by the individual	Standard operating procedure states this specifically	Reduced

Sign Off

Information Governance Representative	
Name	
Job Title	
Signature	
Date	

Caldicott/SIRO	
Name	
Job Title	
Signature	
Date	

Lead/Project Manager	
Name	
Job Title	
Signature	
Date	

What are the grounds for processing personal/ personal sensitive data?

Data Protection Act – Principle 2

What are the Conditions for Processing?

The conditions for processing are set out in Schedules 2 and 3 to the Data Protection Act. Unless a relevant exemption applies, at least one of the following conditions must be met whenever you process personal data:

Schedule 2

- The individual who the personal data is about has consented to the processing.
- The processing is necessary in relation to a contract which the individual has entered into because the individual has asked for something to be done so they can enter into a contract.
- The processing is necessary because of a legal obligation that applies to you (except an obligation imposed by a contract).
- The processing is necessary to protect the individual's "vital interests". This condition only applies in cases of life or death, such as where an individual's medical history is disclosed to a hospital's A&E department treating them after a serious road accident.
- The processing is necessary for administering justice, or for exercising statutory, governmental, or other public functions.
- The processing is in accordance with the "legitimate interests" condition.

What is the legitimate interests condition?

The Data Protection Act recognises that you may have legitimate reasons for processing personal data that the other conditions for processing do not specifically deal with. The "legitimate interests" condition is intended to permit such processing, provided you meet certain requirements.

The first requirement is that you must need to process the information for the purposes of your legitimate interests or for those of a third party to whom you disclose it.

The second requirement, once the first has been established, is that these interests must be balanced against the interests of the individual(s) concerned.

The "legitimate interests" condition will not be met if the processing is unwarranted because of its prejudicial effect on the rights and freedoms, or legitimate interests, of the individual. Your legitimate interests do not need to be in harmony with those of the individual for the condition to be met. However, where there is a serious mismatch between competing interests, the individual's legitimate interests will come first.

Finally, the processing of information under the legitimate interests condition must be fair and lawful and must comply with all the data protection principles.

What Conditions need to be met in respect of personal sensitive data?

At least one of the conditions must be met whenever you process personal data. However, if the information is sensitive personal data, at least one of several other conditions must also be met before the processing can comply with the first data protection principle. These other conditions are as follows

What is the legitimate interests condition?

Schedule 3

- The individual who the sensitive personal data is about has given explicit consent to the processing.
- The processing is necessary so that you can comply with employment law.
- The processing is necessary to protect the vital interests of:
  - The individual (in a case where the individual's consent cannot be given or reasonably obtained), or
  - another person (in a case where the individual's consent has been unreasonably withheld).
- The processing is carried out by a not-for-profit organisation and does not involve disclosing personal data to a third party, unless the individual consents. Extra limitations apply to this condition.
- The individual has deliberately made the information public.
- The processing is necessary in relation to legal proceedings; for obtaining legal advice; or otherwise for establishing, exercising or defending legal rights.
- The processing is necessary for administering justice, or for exercising statutory or governmental functions.
- The processing is necessary for medical purposes, and is undertaken by a health professional or by someone who is subject to an equivalent duty of confidentiality.
- The processing is necessary for monitoring equality of opportunity, and is carried out with appropriate safeguards for the rights of individuals.

In addition to the above conditions – which are all set out in the Data Protection Act itself – regulations set out several other conditions for processing sensitive personal data. Their effect is to permit the processing of sensitive personal data for a range of other purposes – typically those that are in the substantial public interest, and which must necessarily be carried out without the explicit consent of the individual.

Examples of such purposes include preventing or detecting crime and protecting the public against malpractice or maladministration. A full list of the additional conditions for processing is set out in the Data Protection (Processing of Sensitive Personal Data) Order 2000 and subsequent orders.

Common Law Duty of Confidentiality

The general position is that, if information is given in circumstances where it is

expected that a duty of confidence applies, that information cannot normally be disclosed without the data subject's consent.

The four sets of circumstances that make disclosure of confidential information

lawful are:

- where the individual to whom the information relates has given consent
- where disclosure is in the overriding public interest;
- where there is a legal duty to do so, for example a court order; and
- where there is a statutory basis that permits disclosure such as approval under Section 60 of the Health and Social Care Act 2001.

Therefore, under common law, a healthcare provider wishing to disclose a patient's personal information to anyone outside the team providing care should first seek the consent of that patient.

Where this is not possible, an organisation may be able to rely on disclosure being in the overriding public interest. However, whether a disclosure is in the public interest is not a decision to be taken lightly.

The judgement to be made needs to balance the public interest in disclosure with both the rights of the individual[s] concerned and the public interest in maintaining trust in a confidential service. Solid justification is therefore required to breach confidentiality and any decision to disclose should be fully documented.

References

Privacy Impact Assessments – The Information Commissioners Office
http://www.ico.gov.uk/for_organisations/topic_specific_guides/pia_handbook.aspx.

Redmoor Health