Data Protection and Confidentiality Policy

Review date	February 2023, or sooner if changes required
Date of issue	February 2020
Applicable to	All employees, staff on honorary contracts, volunteers and third party contractors
Responsible	Chris Hughes – HR Director

7 Poole Road, Bournemouth, Dorset, BH2 5QR

Shore Medical

RELEVANT TO

1.1 This policy is relevant to all employees of Shore Medical, including staff on honorary contracts, volunteers and third party contractors who process person identifiable information.

2. INTRODUCTION

2.1 This Policy is required in order to inform on the lawfulness and security of personal information, in line with the General Data Protection Regulation 2016, the Data Protection Act 2018 and Common Law Duty of Confidentiality.

2.2 This Policy provides staff with guidance on processing information in accordance with the principles and legal obligations of the Data Protection Act 2018, Confidentiality NHS Code of Practice, Caldicott Report 1997, Caldicott Review 2013 and National Data Guardian's Review on Data Security, Consent and Opt-Outs.

2.3 This Policy also encompasses the Records Management Code of Practice for Health and Social Care 2016, which sets out the legal and professional responsibility of all staff in relation to the creation, use, storage and disposal of records in the performance of their duties.

2.4 Staff should be aware that all records are public records, including email and may be subject to Subject Access Requests and Freedom of Information requests.

3. SCOPE

3.1 This policy aims to inform staff of appropriate use of personal information and their responsibilities.

4. PURPOSE

4.1 The purpose of this policy is to:

- promote best practice in the processing of personal identifiable data;
- ensure that all staff are appropriately trained in the management of personal identifiable data;
- outline the procedure for reporting and investigating suspected breaches of confidentiality and/or loss or theft of personal data;
- provide assurance to patients, staff and general public that personal identifiable data is processed lawfully and held securely.

5. CONFIDENTIALITY

5.1 During the course of their work staff will routinely have access to patient identifiable information, whether verbal, written or electronic. Everyone working within the

NHS has a legal duty to keep information confidential and such information must not be disclosed or discussed except to authorised personnel on a 'need to know' basis.

5.2 Health care information is collected from patients in confidence and attracts a legal duty of confidence until it has been effectively anonymised. This legal duty, established under common law, prohibits information use or disclosure without consent. Such consent may be explicit but it more likely to be implied, e.g. referring a patient onwards for care from another provider. The common law duty of consent applies only to the information which attracts the common law duty of confidentiality and should not be confused with consent as lawful basis for processing personal information found within the Data Protection Legislation.

5.3 At the time of creating a record, staff should ascertain from the patient which relatives and, friends or carers can receive information regarding their condition and those who they do not give permission to receive information. This should be clearly documented within the patients' health record where required. Where relatives and carers are heavily involved in the patients' care, staff should ascertain to what level they should continue to be informed.

5.4 The Confidentiality NHS Code of Practice states: "*It is extremely important that patients are made aware of the information disclosures that must take place in order to provide them with high quality healthcare. In particular, Clinical Governance and Clinical Audit, which are wholly proper components of healthcare provision, might not be obvious to patients and should be drawn to their attention*." Patient information leaflets and the Organisations Privacy Notice should fulfil the organisations obligation under the Confidentiality NHS Code of Practice as well as the concept of 'Transparency' under Article 5(1)(a) General Data Protection Regulation.

5.5 The disclosure and use of confidential patient information needs to be both lawful and ethical, detailed in s.12 of the Confidentiality Code of Practice. A confidentiality model adapted from the Confidentiality NHS Code of Practice can be found at Appendix C.

5.6 Safeguards that are put in place to help protect confidentiality are commonly referred to as 'Safe Haven Procedures'. Guidance on the secure transfer of information can be found at Appendix D. Where the sharing of information is available through a more secure electronic process, this should be favoured over older, more outdated processes.

6. DATA PROTECTION

6.1 Data Protection legislation is derived from the General Data Protection Regulation (GDPR) 2016/679 and the Data Protection Act (DPA) 2018. This legislation provides the Data Protection principles, lawful bases for processing, subject access rights and transfers of data to third country requirements.

6.2 Article 5(1) of the GDPR provides six data protection principles to be upheld:

a) data shall be processed lawfully, fairly and in a transparent manner;

b) data shall be 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, historical research purposes or statistical purposes shall (in accordance with Article 89(1)) not be considered to be incompatible with the initial purposes;

c) data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which that are processed (data minimisation);

d) data shall be 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;

e) data are kept in a form which permits identification of data subject for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes (in accordance with Article 89(1)) subject to implementation of the appropriate technical and organisational measures required in order to safeguard the rights and freedoms of the data subject;

f) data is processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (integrity and confidentiality).

6.3 Article 89(1) specifies “processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, shall be subject to appropriate safeguards, in accordance with this Regulation, for the rights and freedoms of the data subject”. This requires ensuring that there are technical and organisational measures in place which respect and uphold the concept of data minimisation and where purposes can be fulfilled with data that uses pseudonymisation or other data minimisation techniques, they should be used. Guidance on pseudonymisation and anonymisation techniques can be found in Appendix E.

6.4 Article 5(2) of the GDPR provides that the controller shall be responsible for, and be able to demonstrate compliance with, Article 5(1).

Principle One: Lawful processing

6.5 For processing of personal data to be lawful (Article 5(1)(a)) it must meet one of the requirements within Article 6(1):

a) consent for data to be used for one or more specific purposes;

b) processing is necessary for the performance of a contract to which the data subject is party, or in order to take steps at the request of the data subject prior to entering into the contract;

c) processing is necessary for compliance with a legal obligation to which the controller is subject;

d) processing is necessary in order to protect the vital interests of the data subject or another natural (living) persons;

e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

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

6.6 For processing of special categories of data to be lawful (Article 5(1)(a)) it must meet one of the requirements within Article 9(2):

a) explicit consent for one of more specified purposes;

b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law;

c) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;

d) processing is carried out in the course of legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on the condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside of that body without the consent of the data subjects;

e) processing relates to personal data which are manifestly made public by the data subject;

f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;

g) processing is necessary for reasons of substantial public interest which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and interests of the data subject;

h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health and social care systems and services, or pursuant to contract with a health professional and subject to the conditions and safeguards referred in Article 9(2)(3); (i) Personal data may be processed for such purposes when those data are processed by or under the responsibility of a professional subject to the obligation of professional secrecy under Member state law or established by national competent bodies or by another person also subject to an obligation of secrecy;

i) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Member state laws which provide suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;

j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

6.7 Although 'Consent' is listed as a lawful basis for processing both personal and special categories of data, Recital 43 makes it clear that Public Authorities should not be relying on consent due to the imbalance of power between the data subject and the data controller: *"In order to ensure that consent is freely given, consent should not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller, in particular where the controller is a public authority and it is therefore unlikely that consent was freely given in all the circumstances of that specific situation."*

Principle Two: Specified, explicit and legitimate purposes

6.8 The Practice, as a Data Controller, is required to specify the purposes of processing data e.g. for the provision and administration of Healthcare, what data is to be included and to whom it will be disclosed.

6.9 In doing so, the Practice has to consider the data that it requires and is obliged to notify and register its collection purposes with the Information Commissioner. The current processes that the Practice has registered are Shore Medical to include:

a) staff administration to include the HR management system;

b) accounts and records;

c) health administration and services;

d) research;

e) crime prevention and prosecution of offenders;

f) public health;

g) data matching (to assist the National Fraud Initiative).

6.10 Should any member of staff be processing personal data for any purpose other than those listed then you should immediately inform the Data Protection Officer.

Principle Three: Adequate, relevant and limited to what is necessary

6.11 The minimum amount of data necessary and proportionate for the purpose(s) of processing should be collected

Principle Four: Accurate and up to date

6.12 All reasonable steps should be taken to ensure that data is legible, accurate, complete, timely and complies with the Records Management Code of Practice for Health and Social Care.

Principle Five: Not kept for longer than is necessary

6.13 The Practice Manager is responsible for the overall management and confidential disposal of staff records and should review personnel files regularly and ensure that staff records are maintained and, where relevant, summary files are created confidentially disposing of any information which is no longer required.

6.14 The Practice Manager is responsible for the overall management and confidential disposal of Health Records, in line with the Records Management Code of Practice for Health and Social Care, ensuring that appropriate procedures are in place for the transfer of deducted records.

Principle Six: Appropriate Security

6.15 The Practice has technical safeguards in place, such as secure email, encryption, Anti-Virus products and regular external penetration testing.

7. RIGHTS OF THE DATA SUBJECT

The right of subject access

7.1 Under Article 15 GDPR 2016, Data Subjects have the right of access to information about them held by a Data Controller. A data subject (patient or staff) has the right to request confirmation as to whether information is being processed and if so:

a) the purpose of the processing;

b) the categories of personal data concerned;

c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular any third countries or international organisations;

d) where possible, the envisaged period for which the personal data will be stored and the criteria which determine that period;

e) the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing personal data concerning the data subject or to object to such processing;

f) the right to lodge a complaint with the supervisory body;

g) where the personal data are not collected from the data subject, any available information as to their source;

h) the existence of automated decision-making and if it exists, meaningful information about the logic involved and the significance of the envisaged consequences of such processing.

7.2 This information is contained within the Practice's Privacy Notice.

7.3 Article 15 also provides data subjects with the right to obtain a copy of the personal data undergoing processing and requires a response within one month of the receipt of the request, free of charge, in an intelligible format. The Subject Access Request Procedure for Patient and for Staff can be found in Share point/General/Policies & Protocols/GDPR

7.4 Staff should not be exercising their right of access by using the Practice's clinical or employment systems to view their own records or that of friends and family, and should instead follow the same procedure as any other patient or employee without access to systems.

7.5 Staff should not place pressure on colleagues or use workarounds to try and navigate the system in order to obtain results or appointments faster; this would not only breach data protection principles but would also breach the Practice's NHS Contract. Misuse of information and access to systems in this way would constitute potential misconduct/gross misconduct as per the Practice's Disciplinary Policy and could result in dismissal, prosecution for the individual under s.170 of the Data Protection Act 2018, and potential enforcement / contractual implications for the Practice.

7.6 The period of response for a subject access request can be extended by two further months if necessary where there is, for example, complicated post-processing of information required to make the data intelligible or to identify the data subject. Where the deadline is extended the data subject must be informed, within the original one-month timeframe, with an explanation of the delay.

7.7 Where a request is deemed to be "unfounded or excessive" the controller has the right to refuse an information request or to charge a "reasonable fee" to cover the resulting administrative costs. The data subject should be informed, within the one-month time period, of the reasons for not taking action or for charging a fee. Guidance on unfounded and excessive requests can be found in Appendix F.

7.8 Requests can be refused and/or redacted where granting access would disclose information likely to cause serious harm to the physical or mental health of the patient or another individual and the data subject does not already know the information. Any redactions should be approved by the Caldicott Guardian or the patient's GP. Requests can also be refused and/or redacted where granting access

would disclose information which the Practice is not the data controller of, or information relating to or provided by a third party who could be identified from that information and has not provided consent for the release of the information.

7.9 This does not apply to health professionals who have complied, or contributed to, either the record or the individuals care. Schedule 2, Part 3, Section 17(1) of the Data Protection Act 2018 provides an exemption for the processing of third party personal data where the health data test is met. The Health Data test is met whereby the information in question is contained within a health record and the third party is a health professional who has compiled or contributed to the health record or who, is his or her capacity as a health professional, has been involved in the diagnosis, care or treatment of the data subject. There are also Social Work Data tests and Education Data tests in s.17(2) and s.17(3).

7.10 When considering redacting information, the data subjects rights should be held in the highest regard and removal or redaction should only be used where absolutely necessary.

7.11 Anything written about a patient or employee may ultimately be scrutinised by that patient or employee, therefore all entries into records and communications concerning a particular individual, including emails, should be objective and factual.

7.12 Requests can be made by the individual concerned or their legal representative; a solicitor acting on their behalf, their carer, parent, guardian, or an appointed representative. Where the request is not made by the individual themselves it must be accompanied by either a signed authority from the patient, or evidence of legal representation to take decisions.

7.13 Access rights to deceased records are contained within the Access to Health Records Act 1990 and are available where a personal representative has a legal claim arising from the death of the patient or the death may have been caused by negligence, someone who may be entitled to compensation is allowed access to the records relating to the death.

The right to rectification

7.14 Article 16 GDPR contains the right of rectification. Where a data subject feels that information is incorrect, they have the right to ask for it to be rectified - this right applies to information of fact and not opinion. Incorrect demographic information will be immediately corrected. If the information is of a clinical nature this will ned to be reviewed and investigated by the Practice as a potential breach in Records Management procedures and data quality issues. The investigation will yield one of two outcomes:

a) the Practice deems the information to be correct at the time of recording and the record will not be amended. A statement from the data subject may be placed within the record to demonstrate that they disagree with the information held, and the data subject has the right to appeal to the Information Commissioner;

b) the Practice agrees that the information is incorrect. However, it is not legal to modify or remove information within the record as it represents historical information which may have influenced subsequent events or decisions made. A note will be place into the file which alerts the reader of the inaccuracy and the correct facts. The data subject and the Practice will agree the content of the note together.

The right to be forgotten

7.15 Article 17 GDPR contains the right to be forgotten; this is a limited right with regards to health care and employment information. The legal obligation to retain information as per the Health Records Act 1958 in order to maintain patient safety and continuity of care, as well as upholding our obligations as an employer, take precedent over the data subjects right. Exemptions from the GDPR provisions for Healthcare can be found in Schedule 3 of the Data Protection Act 2018.

7.16 The retention schedules within the Records Management Code of Practice for Health and Social Care 2016 are followed, unless there is another legal obligation to retain information for longer for example, financial records. Information will not be destroyed before the retention period is over. Where a data subject requests the 'right to be forgotten', a note will be placed on their record to indicate that they would like their information disposed of as soon as legally admissible.

The right to restrict processing

7.17 Article 18 GDPR contains the right to restrict processing however, it can only be exercised in the following circumstances:

a) the data subject contests the accuracy of the data;

b) the processing is unlawful;

c) the data subject objects to the processing of their data whilst the data controller seeks to verify the legitimate grounds for continuing processing.

7.18 The right to restrict processing of healthcare data for direct care should not be taken lightly and only in extreme circumstances, having given the data subject the opportunity to meet with a relevant clinician who can properly explain the limited services and treatments available to the data subject.

7.19 Data subjects are allowed to restrict the processing of identifiable data for secondary purposes and should be provided with information on the National Data Opt-Out available on the NHS Digital website.

The right to data portability

7.20 This right only applies where the original processing is based on the data subject's consent or fulfilment of a contract that they are party to, and if the processing is automated. However, in the spirit of the regulations, Subject Access Requests should be provided in a useful electronic format and where possible in a commonly used and machine readable format.

The right to object

7.21 Data subjects can object to specific types of data processing, including direct marketing, processing based on legitimate interests or in the wider public interest, and processing for research or statistical purposes. Once a data subject raises an objection, the data controller should demonstrate the legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise of defence of a legal claim. Until the justification can be provided, processing of personal data must be suspended. The right is aligned with the right to restrict processing and data subjects should be provided with information on the National Data Opt-Out available on the NHS Digital website.

The right to appropriate decision making

7.22 Data subjects have the right "not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning them or similarly significantly affects them". The Practice has not identified any decision-making processes which are solely automated and without human interaction, which produces a legal effect for the data subject.

7.23 All NHS records are Public Records under the Public Records Act 1958. The Organisation will take actions as necessary to comply with all legal statutory and professional obligations

8. THIRD COUNTRY TRANSFERS

8.1 Article 44 GDPR 2016 specifies that any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation, shall take place only if the country of destination has adequate legislation and appropriate safeguards.

8.2 Alongside the United Kingdom, the following countries are all members of the EEA and are safe for secure transfer of personal data by the European Commission:

Austria	Belgium	Bulgaria
Croatia	Cyprus	Czech Republic
Denmark	Estonia	Finland
France	Germany	Greece
Hungary	Iceland	Ireland
Italy	Latvia	Liechtenstein
Lithuania	Luxembourg	Malta
Netherlands	Norway	Poland
Portugal	Romania	Slovakia
Slovenia	Spain	Sweden

8.3 Although these countries have been deemed safe, the UK may find that they are removed from this list after leaving the European Union and may need to amend contracts and provisions. Should this happen, the UK should still be deemed adequate, under Article 45 GDPR 2016, for transfers.

8.4 Article 45 provides for the European Commission to decide countries of adequacy based on their rule of law, access to justice, respect for human rights and fundamental freedoms, relevant legislation regarding public security, defence, national security and public order.

8.5 The following countries have been deemed adequate by the European Commission:

Andorra	Argentina	Canada[1]
Faroe Islands	Guernsey	Israel
Isle of Man	Japan[2]	Jersey
New Zealand	Switzerland	Uruguay
USA[3]		

8.6 Article 46 provides a list of acceptable safeguards for potential third countries of transfer to be tested against. These would need to be considered for any transfers beyond those countries listed above, or those with partial adequacy, due to the lack of federal law regulating data protection and human rights and freedoms:

a) legally binding and enforceable instrument between public authorities or bodies;

b) Binding Corporate Rules;

c) Standard Data Protection Clauses adopted by the European Commission, or Supervisory Authority and approved by the Commission;

d) an approved code of conduct with binding and enforceable commitments of the controllers/processors in the third country;

e) contractual clauses between the controller/processor and the controller/processer/recipient in the third country;

f) provisions inserted into administrative arrangements between public authorities or bodies including enforceable and effective data subject rights.

8.7 For all transfers, appropriate information security and protection should be applied, for example encryption, contractual agreements and information security accreditations/certifications such as ISO27001.

9. OFFENCES AND EXEMPTIONS

[1] Commercial Organisations subject to Canada's Personal Information Protection and Electronic Documents Act
[2] Private Sector Organisations
[3] Subject to EU-US Privacy Shield Framework

Exemptions to Data Protection and Confidentiality

9.1 There are a number of obligations where the Practice should disclose identifiable information such as for the purposes of Crime and Taxation, Prevention of Serious Cross Boarder Health Threats, Prevention of Terrorism and Safeguarding Children and Vulnerable Adults. This list is not exhaustive and if in doubt advice should be sought from the Data Protection Officer and/or the Caldicott Guardian.

9.2 Circumstances where a patients' right to confidentiality may be overridden include:

a) where a patient's life may be in danger or they may not be able to make an appropriate decision;

b) where there is a serious danger to other people and the rights of others supersede those of the patient;

c) where there is a serious threat to a health care professional;

d) where there is a serious threat to the community;

e) other exceptional circumstances based on professional consideration and consultation.

Offences

9.3 It is an offence under s.170 of the Data Protection Act (DPA) 2018 for a person to knowingly or recklessly obtain or disclose personal data without the consent of the controller, to procure the disclosure of personal data to another person without the consent of the controller, or after obtaining personal data, to retain it without the consent of the person who was the data controller at the time the information was obtained. It is a further offence if information obtained in this manner is then sold.

9.4 The Practice, as Data Controller, provides consent for employees to access patient or staff records that require access in order to provide health care, employment advice or otherwise fulfil the duties within their job description. Employees do not have consent from the Practice to use clinical systems to access their own records, or that of friends and family to whom they are not providing direct care. It is a breach of the Data Protection Act 2018 and Practice Policy to access such records without following the formal access procedure may constitutes misconduct/ Gross misconduct under the Practice's Disciplinary Policy which may result in dismissal and in some circumstances prosecution from the Information Commissioners Office.

9.5 It is an offence under s.171 of the DPA 2018 for a person to knowingly or recklessly re-identify information that is de-identified personal data without the consent of the controller responsible for de-identifying the data.

9.6 It is an offence under s.173 of the DPA 2018 for the Data Controller, or a person employed by the controller, to alter, deface, block, erase, destroy or conceal information with the intention of preventing disclosure of all or part of the information that the data subject would have been entitled to receive under subject access.

9.7 It is an offence for a person to ask another person to make a subject access request in order to obtain personal data about that person and staff should be aware that those seeking information may be using deception to gain access to information to which they are not entitled. If in doubt seek advice from your line manager or Data Protection Officer.

9.8 Breaches of the data protection and security which result in the loss of personal data which is likely to result in a high risk to the personal rights and freedoms of the data subject concerned must be reported to the Information Commissioner's Office within 72 hours under Article 33 GDPR 2016.

9.9 The Information Commissioner can take enforcement action against the Practice, including a fine of up to €20,000,000 or 4% of the Practice's global turnover for the breach and a fine of €10,000,000 or 2% of the Practice's global turnover for failure to report a breach within 72 hours. Enforcement may also include an Information Notice, Undertaking or Enforcement Notice. It is an offence to fail to respond to these Notices or fines.

9.10 The Practice may appeal to the independent information tribunal, but if the enforcement action is upheld and the Practice continues to break the principles, this would constitute a criminal offence.

9.11 Accessing, disclosing or otherwise using employee (whether current, prospective or former) or patient (whether current, former or deceased) records without authority is a serious disciplinary offence, which will be dealt with in accordance with the Practice's Disciplinary Procedure and could result in dismissal. Accessing, disclosing or otherwise using employee or patient records without authority may also constitute a criminal offence.

9.12 Disclosure of employee or patient information must be on a need-to-know basis only. Unnecessary disclosure constitutes a breach of confidentiality, which will be dealt with in accordance with the Practice's Disciplinary Procedure and could result in dismissal.

9.13 Breaches of data protection and/or confidentiality must be reported to the GP DPOs using the online Incident Reporting Form and a record kept locally.

10. PRIVACY BY DESIGN AND DATA PROTECTION IMPACT ASSESSMENTS

10.1 Data Protection Impact Assessments (DPIAs), previously known as Privacy Impact Assessments, are tools used to analyse processing of personal identifiable data to help identify and minimise any data protection risks at an early stage. DPIAs look at compliance risks as well as risks to the rights and freedoms of individuals and the potential for harm, either physical, material or non-material by considering the likelihood and severity of any impact or harm.

10.2 The outcome of a DPIA should be integrated back into the project plan, with the outcomes and risks kept under review and re-assessed where changes are made.

10.3 DPIAs are a legal requirement where there is a high risk to data processing and should be used in order to assess new projects, data flows or sharing arrangements,

policies and procedures in order to anticipate and review any potential issues with data protection or confidentiality. They are used to identify possible solutions, drive a privacy focused culture and uphold the concepts of Privacy by Design and Data Minimisation.

10.4 DPIAs are most effective if they are carried out at the initiation and design stage of a project, procedure or change. Key ideas, activities and data sharing need to be identified in order to assess them from a privacy perspective and should be completed before any design stage is completed in order to accommodate any alterations required.

10.5 DPIAs enable a Data Controller to identify any risks to privacy and data protection and reduce those risks, protecting individuals and the organisation's reputation, as well as instilling confidence in the public that the organisation has addressed any privacy concerns with any new projects or procedures. DPIAs also help to anticipate and navigate potential problems, preventing costly changes to projects/procedures.

10.6 GDPR requires a DPIA to be completed where there is:

- systematic and extensive profiling which produce significant effects;
- large scale processing of special categories of data, including criminal offence data, health records and social care records; or
- systematic monitoring of publicly accessible places on a large scale, including audio/video surveillance of public areas.

10.7 The ICO lists a further ten types of processing that automatically require a DPIA:

- new technologies: processing involving the use of new technologies, or a different application of existing technologies;
- denial of service: decisions about individual's access to a product, service, opportunity or benefit which is based to any extent on automated decision-making (including profiling) or involves the processing of special categories e.g. credit checks;
- large scale profiling: any profiling of individuals on a large scale e.g. hardware/software offering fitness/lifestyle monitoring, social media networks, or applications of AI to existing process;
- biometrics: any processing of biometric data e.g. access control/identity verification for hardware/applications, including voice recognition, fingerprint or facial recognition;
- genetic data: any processing of genetic data, other than that processed by an individual GP or health professional for the provision of health care direct to the data subject;
- data matching: combining, comparing or matching personal data obtained from multiple sources e.g. fraud prevention, or monitoring personal use/uptake of statutory services or benefits, or direct marketing;

- invisible processing: processing of personal data that has collected from a source other than directly from the individual, without providing them with a privacy notice;
- tracking: processing which involves tracking an individual's geolocation or behaviour, including but not limited to the online environment e.g. social networks, software applications, hardware/software offering fitness/lifestyle/health monitoring, data processing at the workplace, data processing in the contract of home and remote working;
- targeting of children or other vulnerable individuals: the use of children's personal data or personal data from other vulnerable individuals for marketing purposes, profiling or other automated decision-making, or if you intend to offer online services directly to children such as social networks;
- risk of physical harm: where the processing is of such a nature that a personal data breach could jeopardise the [physical] health or safety of individuals e.g. social care records, or whistleblowing/complaint procedures.

10.8 The member of staff who is leading on the project or procedure has the responsibility for conducting the DPIA and consulting the Data Protection Officer. If there is no involvement or impact on personal data, then a DPIA is not required and an exemption should be documented. Guidance on completing a DPIA and a template DPIA can be found in Appendix G.

10.9 The Data Protection Officer should be consulted when a DPIA is being conducted in full and a completed copy provided for information.

10.10 Where a DPIA has been completed and risks remain unmitigated on a project or procedure which is mandatory, the ICO must been notified with a statement of acceptance of the risks from the Practice's SIRO.

11. CALDICOTT PRINCIPLES AND NATIONAL DATA OPT-OUT

11.1 The Caldicott Guide sets out the issues that staff should consider when handling confidential information relating to patients. It also brings together the principles and standards arising from the review of handling patient information in the NHS undertaken by Dame Fiona Caldicott. The Caldicott principles which should be used to test every use or flow of patient identifiable information to a third party.

11.2 Caldicott Guardians were originally appointed following the Caldicott Report in 1997. A committee, chaired by Dame Fiona Caldicott, produced the report as a response to the need to consider how best to manage confidential patient information. In 2013 the Caldicott review reconsidered the outcomes of this first report and its implications within healthcare.

11.3 The Caldicott Guardian is responsible for overseeing the day to day Confidentiality and Information Sharing issues and co-ordinating and raising awareness of Confidentiality at the Organisation.

11.4 All staff, whether temporary, permanent, volunteers or contractors are responsible for ensuring that they are aware of the Caldicott requirements and for ensuring that they comply with these on a day to day basis. All job descriptions and contracts make explicit references to the need not to disclose confidential information relating to patients or staff, within or outside of the workplace, except in the proper discharge of duties.

11.5 Staff across the NHS routinely collects confidential information from patients for a variety of reasons. The public need to have confidence that this information will be kept confidential and handled appropriately, having consideration of the relevant common law duties and legislation. It is however recognised that it is in the public interest that the NHS uses information collected as part of providing clinical care to ensure the best use of resources. Staff in supervisory or managerial positions will also handle information about staff, which also needs to be protected and used properly.

The Caldicott Principles:

Principle One: Justify the purpose(s) of using confidential information;

Principle Two: Only use confidential information when absolutely necessary;

Principle Three: Use the minimum amount that is required;

Principle Four: Access should be on a strict need to know basis;

Principle Five: Everyone must understand their responsibilities;

Principle Six: Everyone must understand and comply with the law;

Principle Seven: The duty to share information when appropriate can be as important as the duty to protect patient confidentiality.

11.6 In 2016 Dame Fiona Caldicott released her report into Data Security, Consent and Opt-Out. The report included 3 Leadership Obligations, 10 recommendations for Data Security Standards and a consent model for opt-outs of identifiable secondary use data.

11.7 Two strong messages came out of the last report. Firstly, engagement with patients and service users regarding the use of their information will encourage public confidence in the NHS' use of confidential data and reduce the need for patients to repeat themselves or their preferences. Secondly, strong leadership is required in each organisation, led by the SIRO, with an engaged Board and well supported Caldicott Guardian.

Data Security Standards	
1	Upholding the Data Protection Act 1998 (now 2018) Principles
2	Staff understand their responsibilities
3	Annual Training

4	Access controls
5	Process review and Risk Event Reporting
6	Cyber Security and Reporting
7	Continuity Planning
8	No unsupported operating systems in use
9	Cyber Security Strategy
10	IT suppliers to be held to account

Consent Model	
1	You are protected by law
2	Information is essential to high quality care
3	Information is essential for other beneficial purposes
4	You have the right to opt-out
5	Your opt-out will be respected across all NHS organisations
6	Explicit consent is possible for specific projects
7	Opt-outs do not apply to anonymised information
8	Opt-outs do not apply where there is an overriding public interest

11.8 A re-designed 'Data Security and Protection Toolkit' came out of the Data Security Standards recommended above and NHS Digital have launched a National Data Opt-Out of identifiable secondary use information, which all NHS organisations in England will have to uphold by March 2020.

12. CONSENT

Common law consent for medical treatment

12.1 Consent to treatment is the principle that a person must give permission before they receive any type of medical treatment, test or examination. This must be done on the basis of explanation by a clinician. For consent to be valid, it must be voluntary and informed and the individual concerned must have the capacity to make the decision.

12.2 If an adult has capacity to make a voluntary and informed decision to consent, or to refuse a particular treatment, their decision must be respected, even if refusing the treatment would result in their death.

12.3 If an adult does not have capacity to make an informed decision and has not appointed a Lasting Power of Attorney for Health and Welfare, the healthcare professional can make a decision for treatment if they believe it's in the persons' best interest. However, advice and consultation with friends and relatives should be undertaken.

12.4 If they are able to, a child and young person aged 13 or older, may be able to give consent themselves however someone with parental responsibility may need to give consent for a child up to the age of 16 to have treatment.

12.5 Consent can be implied or explicit. Explicit consent may be verbal or in writing, e.g. agreeing to have an X-ray or signing a consent form for a procedure. Implied consent can be given, providing that the individual has understood the treatment, e.g. taking clothing off for an examination or holding an arm out for a blood test.

12.6 Consent should be given to the healthcare professional directly responsible for the patient's current treatment, e.g. to the nurse who will take blood or to the GP prescribing a new medication. If someone is going to have a major procedure, such as an operation, explicit consent should ideally be secured in advance and written.

12.7 There are a few exceptions when treatment may be able to go ahead without the patient's consent, even if they are capable of giving consent:

a) the patient requires emergency treatment to save their life but they are incapacitated for example unconscious. The reasons for treatment should be fully explained once they have recovered;

b) the patient immediately requires an additional emergency procedure during an operation. There has to be a clear medical reason why it would be unsafe to wait to obtain consent and not simply a convenience;

c) the patient has a severe mental health condition, such as schizophrenia, bipolar disorder or dementia, and lacks the capacity to consent to the treatment of their mental health. Treatment for any unrelated physical conditions still require consent;

d) the patient requires hospital treatment for a severe mental health condition, but self-harmed or attempted suicide while competent and is refusing treatment. Under the Mental Health Act 1983, the patient's nearest relative or an approved social worker must make an application for the person to be forcibly kept in hospital, and two doctors must assess the persons condition;

e) there is a risk to public health, for example rabies, cholera or tuberculosis;

f) the patient is severely ill and living in unhygienic conditions. Under the National Assistance Act 1948, a person who is severely ill or infirm and is living in unsanitary conditions can be taken to a place of care without their consent.

12.8 More information around consent for medical treatment can be found on the NHS England website.

Consent as a lawful basis for processing data

12.9 Article 6 GDPR 2016 provides the lawful basis for processing personal data. Article 9 GDPR 2016 provides the lawful basis for processing special categories of data. Article 6(1)(a) and Article 9(2)(a) are consent.

12.10 The conditions for consent are contained within Article 7 and Recital 32, and a Data Controller would need to be able to demonstrate that the data subject has consented to the processing of their personal data.

12.11 Consent to process data should be:

a) a clear affirmative action;

b) freely given;

c) specific;

d) informed;

e) an unambiguous indication of the data subjects' agreement to processing.

12.12 The Practice should not rely on consent to process personal or special categories of data.

12.13 **Article 6(1)(e)** provides: "processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller" which the Practice will largely rely on for the processing of patient personal data.

12.14 **Article 6(1)(b)** provides: "processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract" which the Practice will largely rely on for the processing of employee personal data.

12.15 **Article 6(1)(c) and 6(1)(d)** may also occasionally be relied on to process either patient or employee personal data, depending on the circumstance: **6(1)(c)** *"processing is necessary for compliance with a legal obligation to which the controller is subject.* **6(1)(d)** "processing is necessary in order to protect the vital interests of the data subject or of another natural person"

12.16 **Article 9(2)(h)** provides: "processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health and social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to a contract with a health professional and subject to the conditions and safeguards referred to in Paragraph 3".

12.17 **Para. 3** "Personal data referred to in paragraph 1 may be processed for the purposes referred to in point (h) of paragraph 2 when those data are processed by or under the responsibility of a professional subject to the obligation of professional secrecy under Union or Member State law or rules established by national competent bodies or by another person also subject to an obligation of secrecy under Union or Member State law or rules established by national competent bodies."

12.18 The Practice will largely rely on the above for processing special categories of data, but may, depending on circumstances rely on one of the following lawful bases:

a) **Article 9(2)(b):** "processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject";

b) **Article 9(2)(f):** "processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity";

c) **Article 9(2)(i):** "processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy";

d) **Article 9(2)(j):** "processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject."

12.19 Consent for medical treatment and consent to process identifiable data should not be confused. Please seek further advice or clarification from the GP DPO if required.

13. TRAINING

13.1 All staff will be made aware of their responsibilities towards confidentiality and data protection at their induction. This will be followed up by annual mandatory training via Bluestream. Specific roles may require additional training.

13.2 Successful achievement of compliance with confidentiality and data protection training is dependent upon the input of staff at all levels of the Practice.

13.3 Continuous communications and engagement will run throughout the year through team meetings, the GP DPO newsletter, and Best Practice and Guidance on the intranet.

14. COMMUNICATION/DISSEMINATION

14.1 This Policy will be available to staff on Share point and all staff will be notified of its existence upon starting in post or when the Policy is reviewed and republished.

15. MONITORING COMPLIANCE AND EFFECTIVENESS OF THE POLICY

15.1 Monitoring of overall compliance with Data Protection standards will be completed through annual submission of the Data Security and Protection Toolkit.

15.2 Review of compliance with these standards will be conducted through the annual review of the process.

15.3 The Practice will also use breaches of confidentiality and reported losses of information as a monitoring tool to drive improvements in practice.

16. DOCUMENT REVIEW FREQUENCY AND VERSION CONTROL

16.1 This Policy will be reviewed every three years or earlier if appropriate.

Shore Medical

APPENDIX A

DEFINITIONS, LEGISLATION AND GUIDELINES

Definitions

Personal data: Information relating to an individual or identifiable natural person, who can be identified directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to that physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Special categories of data: Data which concerns the racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.

Genetic Data: Personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question.

Biometric Data: Personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data.

Processing: Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Restriction of processing: The marking of stored personal data with the aim of limiting their processing in future activity.

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

Data Controller: The natural or legal person, public authority, agency or the body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

Data Processor: The natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

Third Party: A natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

Confidentiality: A Duty of confidence arises where one person discloses information to another in circumstances where it is reasonable to expect that the information will be held in confidence, for

example patient to clinician, or employee to manager.

Safe Haven: Either a physical location or an agreed set of administrative arrangements that are in place within the organisation to ensure confidential personal information is communicated safely and securely. It is a safeguard for confidential information which enters, leaves or is transferred within the organisation whether by fax, post, electronically, verbally or by other means.

Filing system: Any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.

Data Protection Impact Assessment: A process which helps assess privacy risks to the individuals in the collection, use and disclosure of information and help identify privacy risks, foresee problems and bring forward solutions.

Data Subject: An identifiable natural person.

Natural Person: Living person.

Information Governance: A framework for handling information in a confidential and secure manner to appropriate ethical and quality standards in a modern health service. It ensures that personal information is dealt with legally, securely, efficiently and effectively.

Information Security: The practice of being protecting information from unauthorised access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction.

Data Security and Protection Toolkit: A framework provided by NHS Digital which comprises the 10 Data Security Standards from the National Data Guardian Data Security, Consent and Opt-Out report 2016 and data protection legislation, to drive and monitor improvements and practice.

Personal data breach: A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Pseudonymisation: The processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and it subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

Legislation and Guidelines

- General Data Protection Regulation 2016;
- Data Protection Act 2018;
- Data Protection (Notification and Notifications Fees) Regulations 2000;
- Data Protection (Notification and Notifications Feeds) (Amendments) Regulations 2001;
- Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019;

- Duty of Confidentiality;
- Confidentiality NHS Code of Practice;
- Records Management Code of Practice for Health and Social Care 2016;
- Public Records Act 1958;
- Human Rights Act 1998;
- Access to Health Records Act 1990;
- Health and Social Care Act 2008 (Regulated Activities) Regulations 2014;
- ICO Guidance on Anonymisation;
- ICO Guidance on Privacy Impact Assessments;
- ISO27001:2013 Information Security Management Framework;
- SCCI1596 Secure Email Standards.

Shore Medical

APPENDIX B

ROLES AND RESPONSIBLITIES

The Information Commissioner

The Information Commissioner is the UK Independent Supervisory Authority for Data Protection and Freedom of Information. The role exists to promote good practice and oversee and enforce compliance with the Data Protection Act 2018 and Freedom of Information Act 2000. The Information Commissioner has the power to impose monetary penalties for a serious breach or misuse of data, and for failure to report such an incident. The ICO can also investigate and issues enforcement notice and act as an independent advisor for consultation.

Data Controller

The Practice is the Data Controller of patient and staff information that it holds and has corporate responsibility for the adoption of internal and external information governance requirements and to meet all statutory and legal obligations.

Data controllers are the **main decision makers**. They make decisions about processing activities and exercise overall control of the personal data being processed and are ultimately in charge of and responsible for the processing *i.e. if you decide what data to process and why, you are a data controller*. A controller can be a company or other legal entity (such as an incorporated partnership, incorporated association or public authority), or an individual (such as a sole trader, partner in an unincorporated partnership, or self-employed professional, e.g. a barrister).

Employees of the controller are **not** processors. As long as they are acting within the scope of their duties as an employee, they are acting as an agent of the controller itself. They are part of the controller, not a separate party contracted to process data on the controller's behalf.

Data Processor

The Practice may engage a data processor to process personal information on its behalf, such as third party contractors. Processors need to have appropriate contractual clauses or an Information Sharing Agreement detailing the data, sharing, storage and destruction processes and obligations.

Data processors **act on behalf of**, and only on the instructions of, the relevant controller. Although a processor may make its own day-to-day operational decisions, it should only process personal data in line with a controller's instructions, unless it is required to do otherwise by law *i.e. if you don't have any purpose of your own for processing the data and you only act on a client's instructions, you are likely to be a processor – even if you make some technical decisions about how you process the data*.

A processor can be a company or other legal entity (such as an incorporated partnership, incorporated association or public authority), or an individual, for example a consultant.

If a processor acts without the controller's instructions in such a way that it determines the purpose and means of processing, including to comply with a statutory obligation, it will be a controller for that processing and will have the same liability as a controller.

Caldicott Guardian

A Caldicott Guardian (CG) is a senior person responsible for protecting the confidentiality of people's health and care information and making sure it is used legally, ethically and appropriately and that

confidentiality is maintained. A CG will balance the need to protect people's confidentiality with the need to protect their welfare by ensuring that information is safely communicated among the various professional teams caring for an individual, sometimes across organisational boundaries.

A CG should **not** be accountable to the SIRO; ideally they should be of equal seniority. A CG should provide leadership and informed guidance on complex matters involving confidentiality and information sharing.

All NHS organisations and local authorities providing social services must have a CG who is required to be registered on the publicly available National Register of CGs.

Senior Information Risk Owner

A Senior Information Risk Owner (SIRO) is an Executive Director or other member of the Senior Management Board of an organisation with overall responsibility for an organisation's information risk policy. The SIRO **should not be the Caldicott Guardian**, as the SIRO should be part of the organisation's management hierarchy rather than being in an advisory role.

The SIRO is accountable and responsible for information risk across the organisation. They ensure that everyone is aware of their personal responsibility to exercise good judgement, and to safeguard and share information appropriately.

The SIRO will be expected to understand how the strategic business goals of the organisation may be impacted by information risks. The SIRO will act as an advocate for information risk on the Board and in internal discussions. The SIRO is responsible for authorising access to national systems, and should be registered on the SIRO register on the ODS webpage.

Data Protection Officer

The General Data Protection Regulation 2016 provides the designation of the Data Protection Officer (DPO) (Article 37), the position of the DPO (Article 38), and the tasks of the DPO (Article 39).

A DPO should be employed by a Data Controller and/or Data Processor where the processing is carried out by a Public Authority or body, except for courts acting in their judicial capacity.

The Data Protection Officer (DPO) should be a person with the relevant skills and knowledge; they advise and inform the controller of their obligations under the legislation, and monitor compliance with the legislation. The DPO is also a point of contact with the Supervisory Authority (the Information Commissioners Office) and with Data Subjects who have concerns over the processing of their data.

All NHS employees

All NHS employees whether clinical or non-clinical are responsible for the records that they created, receive or use during the course of their duties; staff and patient records alike. All employees have an obligation to comply with the principles set out in the Data Protection Act 2018 and Confidentiality NHS Code of Practice, as per their contract of employment.

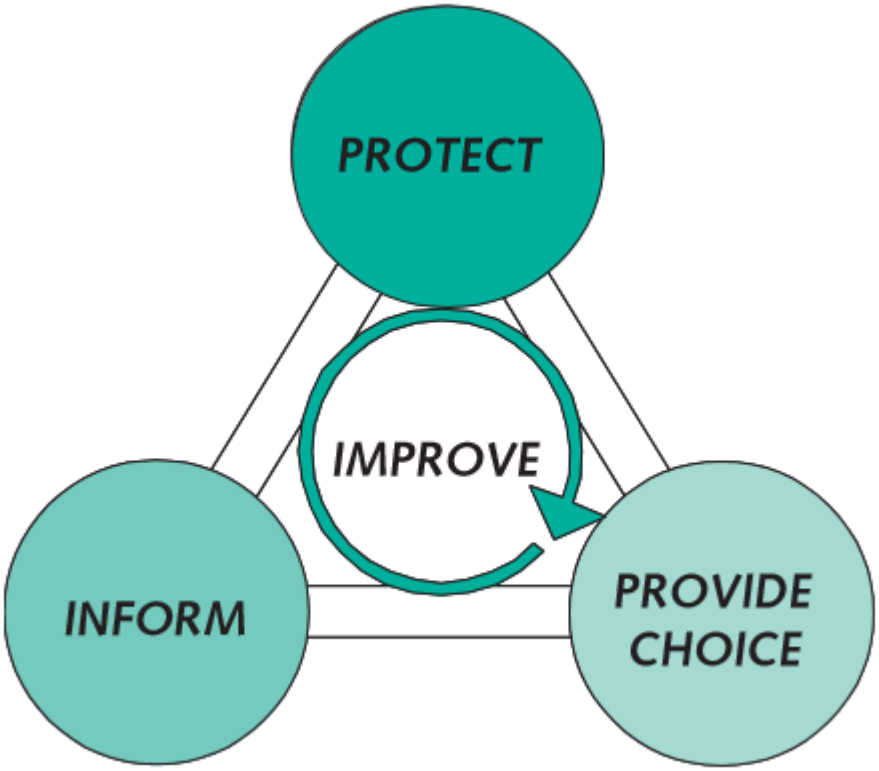
Shore Medical

APPENDIX C

THE CONFIDENTIALITY MODEL (from the Confidentiality Code of Practice)

The model outlines the requirements that must be met in order to provide patients with a confidential service. Record holders must inform patients of the intended use of their information, give them the choice to give or withhold their consent as well as protecting their identifiable information from unwarranted disclosures. These processes are inter-linked and should be ongoing to aid the improvement of a confidential service. The four main requirements are:

- **PROTECT** – look after the patient's information;
- **INFORM** – ensure that patients are aware of how their information is used;
- **PROVIDE CHOICE** – allow patients to decide whether their information can be disclosed or used in particular ways;
- **IMPROVE** – always look for better ways to protect, inform, and provide choice.



Protect Patient Information

Patients' health information and their interests must be protected through a number of measures:

- procedures to ensure that all staff, contractors and volunteers are at all times fully aware of their responsibilities regarding confidentiality;
- recording patient information accurately and consistently;
- keeping patient information private;
- keeping patient information physically secure;

- disclosing and using information with appropriate care.

Shore Medical

Inform Patients Effectively – No Surprises

Patients must be made aware that the information they give may be recorded, may be shared in order to provide them with care, and may be used to support clinical audit and other work to monitor the quality of care provided. Consider whether patients would be surprised to learn that their information was being used in a particular way – if so, then they are not being effectively informed.

In order to inform patients properly, staff must:

- check where practicable that information leaflets on patient confidentiality and information disclosure have been read and understood. These should be available within each NHS organisation;
- make clear to patients when information is recorded or health records are accessed;
- make clear to patients when they are or will be disclosing information with others;
- check that patients are aware of the choices available to them in respect of how their information may be disclosed and used;
- check that patients have no concerns or queries about how their information is disclosed and used;
- answer any queries personally or direct the patient to others who can answer their questions or other sources of information;
- respect the rights of patients and facilitate them in exercising their right to have access to their health records.

Provide Choice to Patients

Patients have different needs and values – this must be reflected in the way they are treated, both in terms of their medical condition and the handling of their personal information. What is very sensitive to one person may be casually discussed in public by another – just because something does not appear to be sensitive does not mean that it is not important to an individual patient in his or her particular circumstances.

Staff must:

- ask patients before using their personal information in ways that do not directly contribute to, or support the delivery of, their care;
- respect patients' decisions to restrict the disclosure or use of information, except where exceptional circumstances apply;
- communicate effectively with patients to ensure they understand what the implications may be if they choose to agree to or restrict the disclosure of information.

Improve Wherever Possible

It is not possible to achieve best practice overnight. Staff must:

- be aware of the issues surrounding confidentiality and seek training or support where uncertain in order to deal with them appropriately.
- report possible breaches or risk of breaches.

Shore Medical

APPENDIX D

SECURE TRANSFER OF INFORMATION

Safe Haven

The term Safe Haven is used to explain either the secure physical location or an agreed set of administrative arrangements that are in place within the organisation to ensure that confidential information is communicated safely and securely. It is a safeguard for confidential information which enters, leaves or is transferred within the organisation whether by fax, email, post or other method of transfer.

Safe Haven locations are those which are lockable or accessible either via coded key pad or electronic access. The room or area should be situated where only authorised staff can enter the location for example, it is not an area which is readily accessible to all members of staff working or visiting the same building or office. If situated on the ground floor any windows should have locks on them and the area should conform to health and safety requirements in terms of fire, theft, flood or environmental damage.

Paper records, including but not limited to health records, staff records and localised records, should be stored in locked cabinets, drawers or rooms when not in use, upholding Regulation 17 of the Health and Social Care Act 2008 (Regulated Activities) Regulations 2014.

Communication in Writing

Written information must be transferred in a sealed envelope and addressed by name to the designated person and clearly marked with "Personal and Confidential – for the named recipient only". All sensitive records must be stored out of view in public areas and not left unsupervised at any time. No personal identifiable information should be visible on any postal package when being transferred by post, and should be secure and contained within a robust envelope or records box.

Electronic Information and Communications

Electronic information should be stored on a password protected computer, on the Practice's Shared Drives. Information shared to local hard drives risk loss and/or corruption which would render the information irretrievable. Laptops and mobile devices should be encrypted and PCs should be located where they are not on view or accessible to unauthorised staff or the general public, with the time-out function enabled.

Computers should be locked when not in use, using the Ctrl, Alt and Delete keys simultaneously or Windows and 'L'. Electronic information which is being transferred using a Compact Disk (CD) or Universal Serial Business Port (USB) memory stick must be encrypted and sent via an appropriate transport or courier company.

Communication by Email or Electronic Transfer

The recipient of email communications must be properly identified by checking the name, organisation and email address.

The Practice has a secure 'mesh' established which enforces TLS encryption to health and social care organisations within Dorset. All other transfers of identifiable data should be done using encryption by placing "[encrypt] " in the subject bar of an email, including the square brackets.

Mass emails being sent to members of the public, staff, patients and/or service users should be avoided where possible and Blind Carbon Copy (BCC) should be used in order to avoid the inadvertent sharing of an individual's email addresses with other individuals, and possible associations with particular conditions or services.

Under no circumstances should identifiable information be transferred via internet email accounts for example, Yahoo, Hotmail, Gmail etc. unless communicating directly with a service user who has given consent for email communications, due to the visibility of email on public networks.

Verbal Communication

A considerable amount of information sharing takes place verbally, often on an informal basis. Care should be taken to ensure that confidentiality is maintained in such discussions. Sensitive telephone calls and discussions should not be held in areas openly accessible to the public. It is important to ensure that confidential telephone discussions are not overheard.

Consideration should be given to the location in which a call is made or received, and a private room should be used for telephone conversations that are highly confidential.

Incoming Calls from a Patient

Care must be taken when receiving calls requesting personal information or when sharing information over the telephone. When speaking with individuals in person over the telephone, it is important to confirm their identity before any confidential or sensitive information is disclosed.

Staff should ensure they gain assurance of the patient's identity by obtaining confirmation of certain personal details, such as:

- name;
- date of birth;
- address and post code;
- appointment dates;
- treatment/clinic details;
- NHS number.

Best practice is to obtain 3 identifiers to confirm the identity of the individual.

Incoming Calls from Relatives and Friends

Information should only be disclosed to next of kin, relatives or friends when the consent of the patient has been obtained. Next of kin do not have any automatic right to confidential patient information. Parents or those with parental responsibility have a right to information about their children unless the child has sought treatment independently of their parents.

Incoming Calls from Other Individuals

Where other individuals such as NHS organisations, health and social care providers, the Police etc. request information about a patient, it is important that they verify their identity and provide evidence that they are authorised to receive the information such as the patient's consent, legal authorisation etc.

A caller's identity can be confirmed by calling them back on an independently verified contact number. This might be a number available on their website, or a call back to the main switchboard, or a call to known and trusted numbers only – not direct lines that are not recognised, or mobile telephones.

If you are unsure as to whether the information should be disclosed, you should take advice from your line manager. Do not disclose any information to the caller – take a phone number, job title

and organisation name, and explain that you will call them back (but only do so on an independently verified contact number, as set out above).

Outgoing Calls

The patient's right to privacy means that when making outgoing calls it is important to speak to the patient directly, unless the patient has provided their consent or it is in their best interests for you to speak to someone else.

Wherever possible, if you think you may need to contact a patient by phone, ask them in advance if they have any preferences:

- Would they prefer to be called at work?
- Would they prefer to be called at home?
- Would they like information to be left with a family member if they know they cannot be contacted directly?
- Are they happy for messages to be left on their answer phones?

These consent preferences should be checked regularly with the patient.

Take care when dialling the number and ensure you have dialled the correct number. If someone other than the patient answers the phone, do not advise the recipient of where you are calling from, simply ask to speak with the patient. If they are not known to the individual who answered the phone, check the number you have dialled with them. If it is the correct number, avoid using alarmist language such as 'it is confidential'. If you have dialled the wrong number, apologise and advise that you have the wrong number.

Answer Machine Messages

There are privacy risks associated with leaving answer phone messages unless the patient has provided their consent to do so.

Where you have consent to leave a message, there is a balance to be struck between respecting the privacy of the patient, not unduly worrying them with an obscure message, and ensuring that the recipient understands that it is a genuine message (e.g. not a scam that is looking to get them to call back a premium rate number).

Staff should take responsibility for considering whether any particular privacy issues exist that could affect whether it is appropriate to leave an answer phone message. Consider the following:

- If you leave an answer phone message, the patient may not be the first to hear it;
- Who else might hear the message?
- Are you sure you have dialled the correct number?
- Will the patient fully understand the content of the message?
- How can you be certain the message has ever been received?
- You may inadvertently breach patient confidentiality because the patient's friends or relatives may not know the patient is receiving health care

Where it is absolutely necessary to leave a message on an answer machine and you do not have consent, staff should take care that they have dialled the correct telephone number. The message

should be brief and simply ask the recipient to call a named member of staff on a given telephone number. The message should not disclose the purpose of the call or identify where the caller is from.

You must be careful when taking messages off answer machines to ensure that the messages cannot be overheard whilst you are playing them back, and that the messages cannot be seen by any unauthorised personnel. They should be passed to the intended recipient as soon as possible.

Fax Communication

Fax communication should be avoided in favour of secure electronic transfers. Fax machines must only be used to transfer personal information where absolutely necessary for the provision of safe clinical care where all avenues of secure electronic transfer have been explored. Approval from the Caldicott Guardian should be sought prior to transferring information via fax.

When sending a fax, a Safe Haven fax number should be obtained from the receiving organisation. If the organisation does not have a safe haven fax machine the follow process should be used to minimise the risk of breach of confidentiality:

- telephone the recipient of the fax and let them know you are about to send;
- ask them to confirm the fax number and wait by the machine whilst you send the fax, where information is particularly sensitive, a test sheet can be sent first to check the number is correct;
- ask for receipt of the fax.

Equipment should, where possible, have a code and password and be turned off out of hours to ensure that fax is not inadvertently received with nobody around. If information does go astray to an unintended recipient:

- complete a risk event report online;
- ask the recipient to return the information if practical, alternatively ask the recipient to confidentially destroy the information;
- discuss with your Practice Manager, SIRO, and Data Protection Officer;
- consider the risk to the person whose personal information has been disclosed or lost and consider informing the individual, including how they can make a complaint if they wish to;
- ensure that the intended recipient receives the information.

Failure to follow safe haven processes could result in breaches in confidentiality, unavailability of data and compromised integrity of the data which may require reporting to the Information Commissioner's Office.

Shore Medical

APPENDIX E

PSEUDONYMISATION AND ANONYMISATION TECHNIQUES

Data Masking

Data masking involves stripping out obvious personal identifiers such as names to create a data set in which no personal identifiers are present.

Variants:

- Partial data removal - results in data where some personal identifiers e.g. name and address have been removed but others such as date of birth remain
- Data quarantining - the technique of only supplying data to a recipient who is unlikely or unable to have access to the other data needed to facilitate re-identification. It can involve disclosing unique personal identifiers, e.g. reference numbers, but not the 'key' needed to link these to particular individuals.

These are relatively high risk techniques because the anonymised data still exists in an individual-level form. Electoral roll data, for example, could be used to reintroduce names that have been removed from the dataset fairly easily. However, this type of data is also relatively 'rich' in terms of allowing an individual to be tracked as part of a longitudinal study.

Pseudonymisation

De-identifying data so that a coded reference or pseudonym is attached to a record to allow the data to be associated with a particular individual without the individual being identified.

Deterministic modification is a similar technique. 'Deterministic' here means that the same original value is always replaced by the same modified value. This means that if multiple data records are linked, in the sense that the same name or address or phone number for example, occurs in all those records, the corresponding records in the modified data set will also be linked in the same way. This facilitates certain types of data analysis.

This is also a relatively high risk technique, with similar strengths and weaknesses to data masking.

Aggregation

Data is displayed as totals, so no data relating to or identifying an individual is shown. Small numbers in totals are often suppressed through 'blurring' or by being omitted altogether.

Variants:

- Cell suppression: if data is from a sample survey then it may be inappropriate to release tabular outputs with cells which contains small numbers of individuals, e.g. less than 30. This is because the sampling error on such cell estimates would typically be too large to make the estimates useful for statistical purposes. In this case, suppression of cells with small numbers for quality purposes acts in tandem with suppression for disclosure purposes
- Inference Control: some cell values, e.g. 1-5, in statistical data can present a greater risk of re-identification. Depending on the circumstances, small numbers can either be suppressed, or the values manipulated. If a large number of cells are affected, the level of aggregation could be changed; the data could be linked to wider geographical areas or age-bands could be widened.
- Perturbation: is a method of disclosure control for tables or counts. It involves randomly adding or subtracting 1 from certain cells in the table.

- Rounding: rounding a figure up or down to disguise precise statistics. E.g. if one table may have a cell value of 10,000 for all people doing some activity up to the present date. However, the following month, the figure in that cell rises to 10,001. If an intruder compares the tables it would be easy to deduce a cell of 1, rounding would prevent this.
- Sampling: in some cases, when very large numbers of records are available, it can be adequate for statistical purposes to release a sample of records, selected through some stated randomised procedure. By not releasing specific details of the sample, data holders can minimise the risk of re-identification
- Synthetic data: mixing up the elements of a dataset, or creating new values based on the original data, so that all of the overall totals and values of the set are preserved but do not relate to any particular individual
- Tabular reporting: a means of producing tabular (aggregated) data, which protects against re-identification

These are relatively low risk techniques because it will generally be difficult to find anything out about a particular individual by using aggregated data. This data cannot support individual level research but can be sufficient to analyse social trends on a regional basis.

Derived data items and banding

Derived data is a set of values that reflect the character of the source data, but which hide the exact original values. This is usually done by using banding techniques to produce coarser grained descriptions of values than in the source dataset, e.g. replacing dates of birth by ages or years, addresses by areas of residence or wards, using partial postcodes or rounding exact figures so they appear in a normalised form.

This is a relatively low risk technique because the banding techniques make data-matching more difficult or impossible. The resulting data can be relatively rich because it can facilitate individual level research but presents relatively low re-identification risk.

Shore Medical

APPENDIX F

UNFOUNDED AND EXCESSIVE SUBJECT ACCESS REQUESTS

What does unfounded mean?

A request may be manifestly unfounded if:

- the individual clearly has no intention to exercise their right of access. For example, an individual makes a request, but then offers to withdraw it in return for some form of benefit from the organisation; or
- the request is malicious in intent and is being used to harass an organisation with no real purposes other than to cause disruption. For example:
    - the individual has explicitly stated, in the request itself or in other communications, that they intend to cause disruption;
    - the request makes unsubstantiated accusations against you or specific employees;
    - the individual is targeting a particular employee against whom they have some personal grudge;
    - the individual systematically sends different requests to you as part of a campaign, e.g. once a week, with the intention of causing disruption.

This is not a simple tick list exercise that automatically means a request is manifestly unfounded. You must consider a request in the context in which it is made, and you are responsible for demonstrating that it is manifestly unfounded. You should not presume that a request is manifestly unfounded because the individual has previously submitted requests which have been manifestly unfounded or excessive or if it includes aggressive or abusive language.

The inclusion of the word "manifestly" means there must be an obvious or clear quality to it being unfounded. You should consider the specific situation and whether the individual genuinely wants to exercise their rights. If this is the case, it is unlikely that the request will be manifestly unfounded.

What does excessive mean?

A request may be excessive if:

- it repeats the substance of previous requests and a reasonable interval has not elapsed; or
- it overlaps with other requests.

However, it depends on the particular circumstances. It will **not necessarily** be excessive just because the individual:

- requested a large amount of information, even if you might find the request burdensome. Instead you should consider asking them for more information to help you locate what they want to receive,
- wanted to receive a further copy of information they have requested previously. In this situation a controller can charge a reasonable fee for the administrative costs of providing this information again and it is unlikely that this would be an excessive request;
- made an overlapping request relating to a completely separate set of information; or

- previously submitted requests which have been manifestly unfounded or excessive.

When deciding whether a reasonable interval has elapsed you should consider:

- the nature of the data – this could include whether it is particularly sensitive;
- the purposes of the processing – these could include whether the processing is likely to cause detriment (harm) to the requester if disclosed; and
- how often the data is altered – if information is unlikely to have changed between requests, you may decide you do not need to respond to the same request twice. However, if you have deleted information since the last request you should inform the individual of this.

What should we do if we refuse to comply with a request?

You must inform the individual without undue delay and within one month of receipt of the request. You should inform the individual about:

- the reasons you are not taking action;
- their right to make a complaint to the ICO or another supervisory authority; and
- their ability to seek to enforce this right through a judicial remedy.

You should also provide this information if you request a reasonable fee or need additional information to identify the individual.

Shore Medical

APPENDIX G

GUIDANCE ON COMPLETING A DPIA AND TEMPLATE FORM

Step 1 – Identify the need for a DPIA

If you are not sure whether or not you need to do a DPIA, ask the Data Protection Officer (DPO) for advice. If you are in any doubt, advice from the ICO is that you should complete a DPIA.

Carry out a screening exercise using the DPIA screening checklist suggested by the ICO. If, following the screening exercise, you decide that you do not need to do a DPIA, you **must** document your decision and the reasons for it (including the advice from the DPO) by keeping an annotated copy of the screening checklist.

Step 2 – Describe the processing

The nature of the processing

You should state in this section what you plan to do with the personal data, including:

- how you collect the data;
- how you store the data;
- how you use the data;
- who has access to the data;
- who you share the data with;
- whether you use any data processors;
- retention periods;
- security measures;
- whether you are using any new technologies;
- whether you are using any new types of processing; and
- which screening criteria you flagged as likely high risk.

The scope of the processing

This is where you document what the processing covers, including:

- what is the personal data you are collecting;
- the volume and variety of the personal data;
- the sensitivity of the personal data;
- the extent and frequency of the processing;
- the duration of the processing;
- the number of data subjects involved; and

- the geographical area covered.

The context of the processing

This is where you should describe the wider picture and incorporate internal and external factors which might affect expectations or impact, including:

- the source of the data;
- the nature of your relationship with the individuals;
- the extent to which individuals have control over their data;
- the extent to which individuals are likely to expect the processing;
- whether they include children or other vulnerable people;
- any previous experience of this type of processing;
- any relevant advances in technology or security;
- any current issues of public concern; and
- whether you comply with any GDPR codes of conduct or GDPR certification schemes;
- whether you have considered and complied with relevant codes of practice.

The purposes of the processing

This is where you document the reason why you want to process the personal data, and should include:

- the intended outcome for individuals;
- the expected benefits for the Practice/PCN or for society as a whole; and
- the legitimate interests of the Practice/PCN, where relevant (you may need to consult the DPO to identify whether there is a legitimate interest).

Step 3 – Consultation process

This section of the DPIA form allows you to set out the consultation process you have used to seek the views of individuals or their representatives. Generally, you should be able to consult individuals in some form. However, if you decide that it is not appropriate to consult individuals, then this decision should be recorded as part of the DPIA, along with a clear explanation. For example, you might be able to demonstrate that consultation would compromise commercial confidentiality, undermine security, or be disproportionate or impracticable.

If the DPIA covers the processing of personal data of existing patients, service users or employees, you should design a consultation process to gather the views of those particular individuals or their representatives. If the DPIA covers a plan to collect the personal data of individuals you have not yet identified, you may need to carry out a more general public consultation process, or targeted research. This could take the form of carrying out market research with a certain demographic, or contacting relevant campaign or consumer groups for their views. If your DPIA decision is not the same as the views of individuals, you must document your reasons for disregarding their views.

If you use a data processor, you may need to ask them for information and assistance. You should consult all relevant internal stakeholders, in particular anyone with responsibility for information security. In some circumstances, you may need to seek legal advice or advice from other independent experts.

Step 4 – Assess necessity and proportionality

This section of the DPIA is where you need to consider whether your plans are actually necessary i.e. do they help to achieve your purpose, or is there any other reasonable way to achieve the same result.

You also need to look at how you will ensure data protection compliance, which is a good measure of necessity and proportionality. To do this, you should document:

- your lawful basis** for the processing i.e. the legal basis for processing the data in order to comply with the Data Protection Act 2018;
- how you will prevent function creep i.e. how you will stop the scope of the project growing beyond the purpose for which it was originally intended;
- how you intend to ensure data quality;
- how you intend to ensure data minimisation i.e. ensure that data collected and processed is not held or further used unless this is essential for reasons that are clearly stated in advance to support data privacy;
- how you intend to provide privacy information (privacy notice) to individuals;
- how you implement and support individuals rights;
- measures to ensure your processors comply; and
- safeguards for international transfers where applicable.

Step 5 – Identify and assess risks

In this section you need to consider the potential impact on individuals and any harm or damage that might be caused by your processing – whether physical, emotional or material. Also look at whether the processing could possibly contribute to:

- inability to exercise rights (including but not limited to privacy rights);
- inability to access services or opportunities;
- loss of control over the use of personal data;
- discrimination;
- identity theft or fraud;
- financial loss;
- reputational damage;
- physical harm;
- loss of confidentiality;

- re-identification of pseudonymised data; or
- any other significant economic or social disadvantage.

You should include an assessment of the security risks, including sources of risk and the potential impact of each type of breach (including illegitimate access to, modification of or loss of personal data).

To assess whether the risk is a high risk, you need to consider both the likelihood and severity of the possible harm. Harm does not have to be inevitable to qualify as a risk or a high risk. It must be more than remote, but any significant possibility of very serious harm may still be enough to qualify as a high risk. Equally, a high probability of widespread but more minor harm might still count as high risk. You must make an 'objective assessment' of the risks. It is worth considering corporate risks as well, such as the impact of regulatory action, reputational damage or loss of public trust.

Step 6 – Identify measures to reduce risk

Against each risk identified, record the source of that risk and then consider options for reducing the risk. This might include, but is not limited to:

- deciding not to collect certain types of data;
- reducing the scope of the processing;
- reducing retention periods;
- taking additional technological security measures;
- training staff to ensure risks are anticipated and managed;
- anonymising or pseudonymising data where possible;
- writing internal guidance or processes to avoid risks;
- using a different technology;
- putting clear data sharing agreements into place;
- making changes to privacy notices;
- offering individuals the chance to opt out where appropriate; or
- implementing new systems to help individuals to exercise their rights.

You should also record whether the measure would reduce or eliminate the risk. You can take into account the costs and benefits of each measure when deciding whether or not they are appropriate.

Step 7 – Sign off and record outcomes

The final step in completing your DPIA is to record what additional measure you plan to take, whether each risk has been eliminated, reduced, or accepted, the overall level of residual risk after taking additional measures, and whether you need to consult the ICO.

You do not always have to eliminate every risk. You may decide that some risks, and even a high risk, are acceptable given the benefits of the processing and the difficulties of mitigation. This would need to be approved by the Senior Information Risk Owner (SIRO). However, if there is still a high risk, you need to consult the ICO before you can go ahead with the processing. The DPO will make

contact with the ICO when required. During consultation, the ICO will review and consider whether; the processing complies with data protection requirements, whether risks have been properly identified and reduced to an acceptable level. The ICO will get back to you within eight weeks, and in complex cases this may be extended to a maximum of 14 weeks.

If you decide not to follow DPO advice, you need to record your reasons. You should also record any reasons for going against the views of individuals or other consultees. You need to keep your DPIA under review, and you may need to repeat it if there is a substantial change to the nature, scope, context or purposes of your processing.

DATA PROTECTION IMPACT ASSESSMENT TEMPLATE

This template is an example of how you can record your DPIA process and outcome. It follows the process set out in our DPIA guidance and should be read alongside that guidance.

You should start to fill out the template at the start of any major project involving the use of personal data, or if you are making a significant change to an existing process. The final outcomes should be integrated back into your project plan.

Controller Details

Name of controller	
Subject/title of DPO	
Name of controller contact /DPO (delete as appropriate)	

Step One: Identify the need for a DPIA

Explain broadly what project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA.

Step Two: Describe the processing

Describe the nature of the processing: how will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? You might find it useful to refer to a flow diagram or other way of describing data flows. What types of processing identified as likely high risk are involved?

Describe the scope of the processing: what is the nature of the data, and does it include special category or criminal offence data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover?

Describe the context of the processing: what is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel in any way? What is the current state of technology in this area? Are there any current issues of public concern that you should factor in? Are you signed up to any approved code of conduct or certification scheme (once any have been approved)?

Describe the purposes of the processing: what do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing – for you, and more broadly?

Step Three: Consultation Process

Consider how to consult with relevant stakeholders: describe when and how you will seek individuals' views – or justify why it's not appropriate to do so. Who else do you need to involve within your organisation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts?

Step Four: Assess necessity and proportionality

Describe compliance and proportionality measures, in particular: what is your lawful basis for processing? Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep? How will you ensure data quality and data minimisation? What information will you give individuals? How will you help to support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfers?

Step Five: Identify and assess risks

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	**Likelihood of harm**	**Severity of harm**	**Overall risk**
	Remote, possible or probable	Minimal, significant or severe	Low, medium or high

Step Six: Identify measures to reduce risks

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5				
Risk	**Options to reduce or eliminate risk**	**Effect on risk**	**Residual risk**	**Measure approved**
		Eliminated reduced accepted	Low medium high	Yes/no

Step Seven: Sign off and record outcomes

Item	**Name/position/date**	**Notes**
Measures approved by:		Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:		If accepting any residual high risk, consult the ICO before going ahead
DPO advice provided:		DPO should advise on compliance, step 6 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:		If your decision departs from individuals' views, you must explain your reasons
Comments:		
This DPIA will kept under review by:		The DPO should also review ongoing compliance with DPIA