Cutlers Hill Surgery

Confidentiality and Information Sharing Protocol

Version	Author	Next Review Date	Notes
V1 (March 22)	Emma Kitcher, DPO	March 23	New protocol that replaces IG08 (info sharing) and IG13 (prescription). Expanded on what is personal confidential information – provided some case studies Included duty of confidentiality / no surprises Faxes should not be used Added Caldicott Principles Included protocol for prescription collection
V1 (March 23)	Emma Kitcher, DPO	March 24	Annual review performed. No changes.
V1 (May 24)	Emma Kitcher, DPO	January 2025	The policies have been extended for the year to accommodate that new legislation is being enacted later in the year.
V1 (Jan 25)	Emma Kitcher, DPO	Feb 26	Annual review. No changes.

Contents

1. INTRODUCTION

Privacy is a concept that emerges from a complex area of law. The three key elements of privacy arise from the Common Law Duty of Confidence / Tort of Misuse of Private Information, Article 8 European Convention of Human Rights (Right to Privacy) and the Data Protection Act 2018 / General Data Protection Regulations (GDPR). This protocol intends to support staff in navigating this framework and encourage lawful, secure and appropriate information sharing.

2. QUICK REFERENCE POINTS

- ✓ You should engage your Caldicott Guardian or DPO to support you with confidentiality queries
- ✓ Personal Confidential Information can include identifiers (like name, email address, but can also be information without identifiers
- ✓ If you are given information that is expected to be kept private, it creates a duty to maintain confidentiality
- ✓ Breaching that duty would be to disclose in an unexpected or unauthorised way
- ✓ Individuals can then bring legal action as a result of damage or distress caused
- ✓ There are circumstances where that duty can be lawfully breached (like public interest, court orders and consent)
- ✓ Routine information sharing should be covered by specific contracts or agreements
- ✓ Ad hoc information sharing should involve careful consideration and support from key roles
- ✓ Do not be pressured or tricked into giving out information – be aware of the rules
- ✓ There are ways in which you can reduce the risk when dealing with paper records, working on the telephone, or sending emails

3. KEY DEFINITIONS

Personal Confidential Information	This term is intended to cover information captured by the Data Protection Act 2018 / GDPR (identifiable information about the living), information covered by the Common Law Duty of Confidence / Tort of Misuse of Private Information and finally, information covered by Article 8 European Convention for Human Rights.

4. SCOPE

See Information Governance Policy for key roles.

All staff, whether management or administrative, who create, receive and use Personal Confidential Information have responsibilities to ensure lawful, secure and appropriate information sharing. Employees have a contractual and legal obligation to read and comply with all company policies and to attend mandatory training to support the appropriate management of information.
The privacy and confidentiality owed to service users, employees, visitors and customers is paramount to maintaining strong relationships with our stakeholders and protecting both those individuals and our reputation.

5. KEY LEGISLATION / FRAMEWORK

Data Protection Act 2018 / General Data Protection Regulations (GDPR
This legislation protects Personal Data (information which identifies or could identify a living individual).

Common Law Duty of Confidence / Tort of Misuse of Private Information
This common law protects information which a ‘reasonable person’ would expect to remain private. This might include financial / contract information or information about the deceased.

Article 8 European Convention of Human Rights (Right to Privacy)
This inherent human right determines that citizens have a right to have their information and family life protected from arbitrary interference from the state – i.e. public bodies or those working on behalf of public bodies.

6. WHAT IS PERSONAL CONFIDENTIAL INFORMATION?

- This term is intended to cover information captured by the Data Protection Act 2018 / GDPR (identifiable information about the living), information covered by the Common Law Duty of Confidence / Tort of Misuse of Private Information and finally, information covered by Article 8 European Convention for Human Rights.

- Personal Confidential Information may be held on paper, USB sticks, computer file or printout, laptops, tablets, mobile phones or even heard by word of mouth or telephone.

- Personal Confidential Information includes information that contains the following identifiers

  - Name
  - Email address
  - Passport number
  - Digital identity
  - Birthplace
  - Telephone number
  - Home address
  - National identification / NHS Number
  - IP address
    Date of birth
  - Login, screen name, nickname, or handle

  - Country, state, postcode
  - Gender or race
  - Grades, salary, or job position
  - Health records
  - Age (particularly if extreme i.e. very old)
  - Name of the school they attend or workplace
  - Criminal record
  - Web Cookie / IP address

- It is important to note that the absence of identifiers does not mean that information is not Personal Confidential Information.

Example

A spreadsheet of patients entitled “Cancer Patients of Old Town, Eastbourne” has been produced. The names, addresses and NHS Numbers have all been removed. But the age and conditions have been left in. One patient is 99 years old. He may be the only 99-year-old in this small town and so is immediately identifiable.

Example

A spreadsheet of patients that is very large indeed and covers the whole country is produced. The names, addresses, age and NHS Numbers have all been removed. But the conditions have been left in. One patient has a very rare condition that only 4 people worldwide have been diagnosed with, and he has been in the media as a result. He is immediately identifiable and now, the other health information recorded in the spreadsheet can easily be linked with his identity.

Example

An employee spreadsheet is produced that lists salaries against each staff member in each department but does not include their name or job title. It shows that there are 20 people in the sales team and their salaries range from £18,000 to £40,000. However, the Equality and Diversity Team only has two employees. The Lead and the Assistant. It would be clear which salary related to which employee in this scenario.

- Some information is more sensitive and requires additional care and requires a specific lawful basis to handle it. This is because, if accessed by an unauthorised individual, this type of information has the potential to cause damage or distress to the data subject.

  - ✓ racial or ethnic origin
  - ✓ political opinions
  - ✓ religious or similar beliefs
  - ✓ trade union membership
  - ✓ Biometrics such as fingerprints
  - ✓ political opinions
  - ✓ physical or mental health or condition
  - ✓ sexual life
  - ✓ Commission (actual or alleged) or proceedings for an offence
  - ✓

- Non-person-identifiable information can also be considered confidential. For example, confidential business information such as financial reports; and commercially sensitive

information such as contracts, trade secrets, procurement information. This information should also be treated with care.

7. THE DUTY OF CONFIDENTIALITY / NO SURPISES

- In order for a duty of confidentiality to exist, an individual has disclosed information to you (or it was obtained from a third party) that a reasonable person would expect to remain confidential.
- Now that a duty exists, you can be held legally accountable for 'breaching' that duty.
- This means that if you disclose that information in an 'unauthorised' or 'unexpected' way, the individual can bring legal action for the damage caused as a result.
- There are times when you can legally 'set aside' or breach your duty of confidentiality for example;

  - ✓ when the individual gives their consent
  - ✓ or it is in the public interest
  - ✓ or to protect someone from harm
  - ✓ Or the court has ordered it
  - ✓ Or the individual reasonably expects the disclosure

- When considering activities or possible disclosures that involve Personal Confidential Information, consider;
  - ✓ Is this something we already list in our privacy materials?
  - ✓ Is this something that the average individual would expect me to do?
  - ✓ Would a reasonable person be 'highly offended' if I did not contact them before I do this?
- If the answer to any of the above questions is 'no', refer the activity to your Data Protection Officer who can assist with raising awareness.

- The concept of no surprises doesn't mean that we ask for consent every time we undertake activity with Personal Confidential Information.

Example:

We are required to disclosure information about a person that poses a threat to the public. We believe that making them aware of the disclosure could trigger the threat we are trying to manage. We do not tell the individual or obtain consent. However, we already note in our privacy materials that we will make these kinds of disclosures. The average, reasonably person expects these types of disclosures and would not be 'highly offended' at the concept of protecting the public. Therefore, there are "no surprises".

- Informing individuals about how their information is used supports their human rights. We all have a right to feel a sense of control over our lives. Involving individuals through transparency and engagement supports this control and autonomy

8. CONSIDERATIONS WHEN SHARING

- ✓ Take care to ensure that information is only shared with the appropriate people in appropriate circumstances
- ✓ When sharing in a complex or non standard scenario, use Appendix A and B to consider all the elements and manage the risk
- ✓ Care must be taken to check there is a legal basis for disclosure before releasing it. The lawful basis will be recorded in the Information Sharing Agreement or Protocol.
- ✓ If it is possible, de-identify or anonymise the data before disclosure
- ✓ De-identifying or pseudonymising the data means removing any direct identifiers (name, email address) and possibly leaving a reference number or code (i.e.NI Number, postcode, NHS Number). This is still personal data, but it reduces the risk.
- ✓ Anonymisation means removing any opportunity that the data could be linked back to a particular individual. Gain support from the DPO to establish whether data is, in fact, anonymised.
- ✓ When personal information is being shared routinely between the practice and other organisations – the Information Sharing Protocols or Agreements mentioned above will support your sharing decisions and identify best practice.

- ✓ When you are required to share personal information for a ‘one off’ purpose, you should consider the potential benefits and risks, either to individuals or society, of sharing the data. You should also assess the likely results of not sharing the data and apply common sense.

- With any request to share Personal or Sensitive Personal Confidential Information outside of usual practice or outside of the country, always speak with the Caldicott Guardian or Data Protection Officer to confirm the approach.

9. ROUTINE SHARING WITH THIRD PARTIES

- All routine sharing of Personal Confidential Information should be covered by an Information Sharing document.
- When the sharing is between two Data Controllers for example;
  - ✓ A GP practice and a hospital
  - ✓ A company and their solicitor
- There should an Information Sharing Agreement in place that identifies why and how information will be shared and the measures taken to protect it.

- Where the sharing is between Cutlers Hill Surgery and a provider who is processing Personal Confidential Information on their behalf, there should be a Processing contract in place that meets with the requirements of GDPR Article 28 and s 59 DPA 2018.
- See Appendix D.

- Where a third party is not processing Personal Confidential Information on the Cutlers Hill Surgery’s behalf but may come in to contact with such data incidentally (such as a cleaner or contractor), they must have signed a confidentiality agreement.

10. MAINTAINING A CONFIDENTIAL ENVIRONMENT

- Secure or confidential operational environment exists when there is either a secure physical location or an agreed set of administration arrangements in place within the Cutlers Hill Surgery that ensure Personal Confidential Information is handled and shared safely and securely.

- It is a safeguard for privacy for all the stakeholders of Cutlers Hill Surgery. Any members of staff handling Personal Confidential Information, whether paper based or electronic must adhere to the principles of a secure / confidential environment. The guidelines below identify how Cutlers Hill Surgery maintains a SOE and so it is crucial that all staff are aware of and comply with this Procedure.

11. TELEPHONE ENQUIRIES

- A service user, staff member, member of the public or partner organisation may telephone us, for example to discuss an individual, report a problem or to access some information.
- Some people attempt to gain information from organisations illegally by deception.
- This practice is known as Voice Phishing or “blagging” and is part of an illegal trade in Personal Confidential Information. An individual with a legitimate request will be open about their activity and will not need to resort to Voice Phishing.
- You should not disclose any information unless you are sure they are the person they say they are and need access to the information as part of their job role. If in any doubt, do not disclose the information and speak to the Information Governance Lead or Data Protection Officer.

- If a request for personal information is made by telephone, always satisfy yourself as to the identity of the caller by;

  - ✓ confirming the identity of the individual
  - ✓ if in doubt as to whether the information should be disclosed tell the caller you will call them back and take advice from your manager
  - ✓ confirm the reason for the request and only share the minimum necessary information, particularly information related to sensitive topics
  - ✓ ensure you keep a record of your name, date/time of disclosure, the reason for it, who authorised it and the contact details of the recipient

- Remember that even the fact that an individual is known to Cutlers Hill Surgery is confidential. If in doubt, consult the Data Protection Officer.

12. REQUESTS FROM THE INDIVIDUAL, THE POLICE OR MEDIA

- Liaise with DPO for such requests.

13. DISCLOSURE TO OTHER EMPLOYEES

- In line with the 'Need to know' principle, Personal Confidential Information should only be released to individuals that have a genuine, identified business need.
- Don't be coerced into giving out Personal Confidential Information. If in doubt, check with a senior member of staff.

14. CARELESSNESS

- Do not talk about patients or staff in public places or where you can be overheard
- Do not discuss patients' sensitive information with friends or colleagues. Remember, even if you omit names – someone may know that person
- Do not leave any medical or staff records or confidential information lying around unattended
- Make sure that any computer screens, or other displays of confidential information i.e. whiteboards, cannot be seen by anyone who does not need to know. Ensure that screens are locked when away from your desk.

15. INTERNAL AND EXTERNAL POST

- Maintain a clear desk policy and undertake regular checks where possible to identify errors or potential breaches.
- Staff should not copy or amend existing letters – use a fresh template to avoid errors.
- High volume or bulky material must only be transported in approved boxes and never in dustbin sacks or other containers and must be locked away until collected by an approved carrier.
- Personal Confidential Information should always be labelled as Private & Confidential on the envelope and letters should be addressed to an individual rather than a team where possible.
- Always provide a return address and ensure the packaging is robust.

16. USE OF FAXES

- Faxes should not be used for Personal Confidential Information.

17. EMAILING

- Personal Confidential Information must be sent using a secure email service such as NHS Mail
- If, for any reason this is not possible, it should be sent in a password protected spreadsheet, with the password being given to the recipient separately by phone or use the NHS Digital Secure method detailed in the Disclosures protocol.
- Always double check you are sending the email to the correct recipient.
- Regularly check / update your distribution list to ensure copies are not sent to staff who have left, moved to another service or no longer require the information
- Where possible, telephone the recipient of the e-mail to let them know you are going to send Personal Identifiable Information
- When emailing information to several members of the public always use bcc so that their email addresses are not visible to one another.

18. PAPER RECORDS

- When printing Personal Confidential Information use the ‘locked print’ facility. Departments that are printing any Personal Confidential Information should have a limited access printer
- Never leave Personal Confidential Information on the printer / photocopier
- If you find unclaimed personal information in the printer / photocopier, you must complete an information incident form.
- Clear your desk at the end of each day, keeping all portable records containing Personal Confidential Information in recognised filing and storage places that are locked at times when access is not directly controlled or supervised
- Paper records must always be kept locked away when unattended. This includes when the building is locked for the evening.

19. ABUSE OF PRIVILEGE

- Staff are strictly forbidden to access their own Personal Confidential Information unless specifically authorised to do so. This includes looking at your own HR files.
- Staff are forbidden to access any personal information relating to public figures, colleagues, friends or relatives unless they have a legitimate reason to do so as part of their employment responsibilities.
- Such activity would be a breach of the Computer Misuse Act 1990 and / or Data Protection legislation.
- If you wish to request a copy of your Personal Confidential Information refer to Information Access and Rights Procedure.

20. CALDICOTT PRINCIPLES

- The following principles can help guide you to make lawful, considered decisions when it come to sharing patient data in particular;

Principle 1: Justify the purpose(s) for using confidential information
Every proposed use or transfer of confidential information should be clearly defined, scrutinised and documented, with continuing uses regularly reviewed by an appropriate guardian.

Principle 2: Use confidential information only when it is necessary
Confidential information should not be included unless it is necessary for the specified purpose(s) for which the information is used or accessed. The need to identify individuals should be considered at each stage of satisfying the purpose(s) and alternatives used where possible.

Principle 3: Use the minimum necessary confidential information
Where use of confidential information is considered to be necessary, each item of information must be justified so that only the minimum amount of confidential information is included as necessary for a given function.

Principle 4: Access to confidential information should be on a strict need-to-know basis

Only those who need access to confidential information should have access to it, and then only to the items that they need to see. This may mean introducing access controls or splitting information flows where one flow is used for several purposes.

Principle 5: Everyone with access to confidential information should be aware of their responsibilities

Action should be taken to ensure that all those handling confidential information understand their responsibilities and obligations to respect the confidentiality of patient and service users.

Principle 6: Comply with the law

Every use of confidential information must be lawful. All those handling confidential information are responsible for ensuring that their use of and access to that information complies with legal requirements set out in statute and under the common law.

Principle 7: The duty to share information for individual care is as important as the duty to protect patient confidentiality

Health and social care professionals should have the confidence to share confidential information in the best interests of patients and service users within the framework set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies.

Principle 8: Inform patients and service users about how their confidential information is used

A range of steps should be taken to ensure no surprises for patients and service users, so they can have clear expectations about how and why their confidential information is used, and what choices they have about this. These steps will vary depending on the use: as a minimum, this should include providing accessible, relevant and appropriate information - in some cases, greater engagement will be

- You can also approach your organisation’s Caldicott Guardian to help you navigate these decisions.

21. DISPENSING PRESCRIPTIONS

- This section is included because there are particularly high levels of confidentiality breaches associated with this activity.
- It is necessary to ensure that the identity of the individual collecting information (either the patient or their representative) is confirmed through “reasonable means” and that the risk of a breach of personal data / confidentiality is balanced through a proportionate response that does not result in a significant increase in burden on the organisation.
- A Risk Assessment has been completed at Appendix A that underpins the proposed approach below.

  - ✓ Individual presents for prescription
  - ✓ Ask if collecting for themselves or another
  - ✓ Ask patients name, DOB & Address
  - ✓ View ID if not the patient
  - ✓ Get representative to print name and sign back of kept prescription form

22. IN PERSON COLLECTION – OTHER ITEMS (I.E. COLLECTING SAR PAPERWORK)

- Ask for patients’ name, DOB and address
- Ask if th ey are the patient or picking up on behalf of the patient
- If patients’ representative, ask to view ID and note the representative’s name.
- Check name, DOB and address on information to be handed over.
- Handover the information if it is the correct patient
- Update relevant log to note who picked up the information.
- For example, if it was a subject access request being picked up – on your SAR log you should note either ‘patient picked up on [insert date] or [name] picked up on [insert date]

23. APPLICATION AND AUDIT

Compliance with this protocol will be audited and the results fed into the Plan, Do, Check, Act Cycle described in the Information Risk and Audit Protocol.

- ✓ Staff must confirm that they have read and understood this protocol
- ✓ This protocol will be reviewed annually or sooner in the event of significant learning or change
- ✓ This protocol should be read in conjunction with the other protocols in the Data Protection and Security policy suite
- ✓ Further relevant guidance can be found in the Disclosures and Access Protocol

24. APPENDIX A: SHARING SCENARIOS

Non-Standard Sharing of Personal Confidential Information

Lawful Basis	*Objective*	*Minimisation*	*Information*	*Re*
Is the sharing covered by the terms and conditions? Have you obtained seperate consent? Is it in the public interest?	You should have a clear objective for the sharing. This will allow you to work out what data to share and with whom.	Always share the minimum data necessary to achieve the identified purpose. Could any identifiers be removed before sharing?	Provide information about any third parties, what the information will be used for and the impact of not consenting.	Ensure o who need Think abo ensure t party appr

Obtaining Consent to Process / Share Personal Confidential Information

Power Imbalance	*Clarity*	*Accessibility*	*Information*	*Withdrawal*
There must be a genuine choice and control. Where delivery of health services is conditional on consent to share - it creates a power imbalance.	Obtain a very clear and specific statement of consent such as a written declaration or ticking a box. Be specific, granular, clear and concise about what is being consented to.	Consider those with different levels of understanding (disabilities, illiteracy, diverse cultural conditions and language differences).	Provide information about any third parties, what the information will be used for and the impact of not consenting.	Provide information about how to withdraw consent - this must be as easy as giving it.

Sharing Personal Confidential Information in the best interests of the Individual

Consent	Clinican	Sharing Considerations	Wishes	Family / Carers	Sharing Log
Is the patient physically / mentally unable to provide consent? See Mental Capacity Act 2005.	A 'best interest' decision is ideally made by the healthcare professional concerned.	Sharing will be in line with the Non-standard sharing diagram at Appendix A	Any decision will need to take into account any sharing preferences already expressed by the individual.	The decision may be informed by the views of family / carers.	The decision will be recorded on the Non-standard Sharing Log

Sharing Personal Confidential Information in the public interest

Consent	Public Interest	Balancing
Is the patient unable or unwilling to provide consent? Would consent prejudice the public interest i.e. put the public at risk?	Any public interest found in bypassing privacy and confidentiality must be established.	The public interest in disclosure must be deemed to be greater than the maintaining confidentiality.

25. APPENDIX B: NON-STANDARD INFORMATION SHARING TEMPLATE

What are the details of the sharing request (no personal data)?	
Do you have a clear objective for disclosure? This will allow you to determine what needs to be shared and with whom.	
What is the lawful basis under Data Protection legislation? For example, public interest, court order, delivery of healthcare.	

On what basis is the duty of confidentiality set aside? For example, public interest, court order, the individually 'reasonably expects' such a disclosure	
Does the disclosure represent a lawful interference with the individuals' rights to privacy under the European Convention of Human Rights? For example, it is lawful, it is in order to protect health and morals.	
Identify the public interest factors for disclosure that outweigh the public interest in maintaining confidentiality. For example, public interest in protecting individuals from harm, public interest in observing the rights of individuals to access their information, the public interest in prevention and detection of crime.	
If the request is a subject access request made on or by the individual, please consult the Information Access and Rights Protocol.	
Has a review been carried out to ensure that the minimum necessary data has been requested for the lawful purpose? Could any identifiers be removed?	
Consider whether the individual has or will be notified about the disclosure. If this would prejudice the purpose in some way – document it here.	
Consider the specific individual that the information should be disclosed to and ensure there is a 'need to know'	
Has a review been carried out to ensure that the information being requested is legitimate and necessary for the lawful purpose?	
Consider the methods for sharing information in terms of their security and safeguards in place.	
Outcome	
Sharing to Safeguard Children	

Which section of the Children Act is the request for information being made to support? i.e. s17, s47	
Does the requestor **genuinely and reasonably** believe that it is desirable to share information to protect children?	
Has consent been obtained and if not, would doing so prejudice the lawful purpose?	
Would the sharing of information be in the public interest?	
Is the Common Law Duty of Confidentiality lawfully set aside because the information is necessary to discharge a legal duty under Children Act?	
Is it believed that sharing the information would support protection of the individuals Article 3 right to be protected from '*torture or … inhuman or degrading treatment or punishment'?*	
Would sharing the information support protection of the individuals Article 2 right to life*?*	
Is it believed that sharing the information would represent a **lawful and proportionate** interference with the child's Article 8(1) right to privacy?	
Is it believed that sharing the information would represent a lawful and proportionate interference with **other individuals'** Article 8(1) right to privacy?	
Are both / all parties signatories to a Multi-Agency Safeguarding Information Sharing Agreement?	
Has a review been carried out to ensure that the minimum necessary data has been requested for the lawful purpose?	
Has a review been carried out to ensure that the information being requested is legitimate and necessary for the lawful purpose?	

Outcome	

26. APPENDIX C: TRANSFERS OUTSIDE OF THE UK

The countries where data may be transferred without additional assurances are (please still seek support of DPO):

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

The following also have an adequate level of protection for personal data

Andorra	Guernsey	New Zealand
Argentina	Isle of Man	Switzerland
Faroe Islands	Israel	Uruguay
	Japan	
	Jersey	

27. APPENDIX D: PROCESSOR CONTRACT REVIEW TEMPLATE

In line with the requirements of GDPR Article 28 and s 59 DPA 2018, this contract allows Cutlers Hill Surgery to review the contracts in place with Data Processors and ensure they are compliant.

This checklist serves as a first part of the process towards confirming that a contract contains the relevant terms and conditions to allocate Data Protection responsibility and to ensure that appropriate controls are in place to protect Personal Confidential Information

In line with Data Protection Act 2018, the Data Processor acts only on the instruction of the Data Controller, and this MUST be under a legally enforceable contract.

Contract/Supplier Name:	
Synopsis of use of information and types of information used:	
Date Checklist Completed:	
Senior Responsible Owner:	

Required clause/areas covered by contract	Included y/n/NA	Notes/Comments
If possible, please attach or provide a map of data flows, i.e. where information will travel from and to, and what the information might contain		
Is the processor required to provide, on request evidence that they have implemented appropriate technical and organisational measures to protect personal data including storage and transmission of data, business continuity, staff training, auditing, access control and Cyber security?		
Does the contract state that the processor shall not engage another processor without prior specific or general written authorisation of the controller?		
Does the contract set out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller?		
Does the contract stipulate that the Processor processes the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by law and in those cases will notify the Controller?		

Required clause/areas covered by contract	Included y/n/NA	Notes/Comments
Does the contract state that all staff employed by the processor have contracts that include confidentiality clauses and that Personal Data will not be shared with third party unless required to do so by law?		
Does the contract require the Processor to assist the Controller to respond to requests for exercising the data subject's rights i.e. access to information, correction of errors?		
Does the contract require the Processor to assist the Controller in reporting information incidents promptly including where it might be required to contact the data subject?		
Does the contract state what should happen to the data at the end of the contract or in the event of termination such as return of the data or secure destruction?		
Does the contract require the Processor to allow for a comply with audits including inspections conducted by the Controller or a third party engaged by the Controller?		

28. APPENDIX E: DISPENSING PRESCRIPTIONS RISK ASSESSMENT

In assessing the level of risk associated with unidentified individuals collecting prescriptions, the DPO has considered the following;

- The likelihood, given (time, cost, effort), that an individual could gain access to information that might impact on the rights and freedoms of individuals
- The nature of the information that may be accessed inappropriately
- The impact that such a disclosure might have on the rights and freedoms of the data subject

UK GDPR Recital 85 provides that a breach may result in;

physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned.

Assessment

The current authentication process is;

1. Person asks to pick up information about a patient
2. Staff members asks for Name, DOB and / or first line of address

Considered Scenarios

1. The patient has not authorised person to pick up the information on their behalf.
2. Staff give out incorrect patient's information.

The Patient has not authorised person to pick up information on their behalf

In this example, the prescription falls into the hands of someone who doesn't have authority to pick up.

Likelihood	**Low**	Patient would have to be known to the person picking the information up for them to already have personal information such as Name, Date of Birth and / or address
Nature	**Low**	By staff ensuring to ask the questions, such as address and DOB as well as name, the resulting residual risk is assessed to be low. It is conceivable that a determined individual might use this information, in order to pick up a prescription for example; where the individual has personal motives such as coercion and control as part of domestic abuse. However, it stands to reason that contacting the patient each time to confirm that the person collecting is authorised could be disproportionate to the level of risk presented by this potential event. If their intention is fraud by a stranger; the person already has basic demographic information such that it is difficult to see how collection of a person's medical information might benefit them. Additionally, they would have to know there was something ready for collecting and the location.
Impact - Low		
loss of control over their personal data, limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of		It is envisaged that where the patient themselves is not picking up their requested information, the representative has the authority to do so. The addition of further levels of security such as signed patient consent forms or not permitting representatives to collect

pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by obligations of secrecy.	paperwork or prescriptions for them could cause harm to the health of a patient if they rely on others' help.
Mitigations	The responsible staff member should ask for the patients' name, DOB and address. The representative should be asked for ID. Where it is a prescription being collected staff should also have the collector sign and date the back of the script to confirm who collected. This way there is a record of who has collected the prescription to aid in the investigation of any breaches.

Staff give out incorrect patient information

In this example, the prescription / paperwork belongs to another patient, who shares one same identifier.

Likelihood	**Moderate**	Patient / representative is only asked for one identifier and this identifier is the same for multiple patients. Thus, the staff members give out a prescription / paperwork believing it to be for the other patient.
Nature	**Low**	By staff ensuring to ask the questions, such as address and DOB as well as name, this risk is incredibly low. Whilst one identifier, such as name, can be shared by multiple people, and even on a very rare occasion could also share a DOB. It is impossible to imagine a scenario where multiple patients have the same name, DOB and address.
Impact - Moderate		
loss of control over their personal data, limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data		It is envisaged that, where information is being picked up, single identifiers are not enough to ensure the correct information is handed out. Multiple identifiers are needed to ensure this does not happen. Not only does a breach affect the second patient, the first patient is without their medication / information and may have to journey back to the surgery to get this corrected and drop incorrect one off. Even when the surgery offers to deliver, they are still

protected by obligations of secrecy.	inconvenienced having to wait in and, where it is medication, potentially miss a dose of the prescription.
Mitigations	Ask for three identifiers to ensure correct patient. If area is busy and staff member believes they may have misheard, ensure they clarify the request before handing the information over.