Patient Information Collection Protocol

|  |  |  |
| --- | --- | --- |
| Policy Title / Reference | Author | Owner |
| Prescription Collection Protocol | Emma Cooper, DPO | Practice Manager |

|  |  |  |
| --- | --- | --- |
| Version | Revision author | Version comments |
| 1 | Emma Cooper, Kafico Ltd | Jan 19 - New Draft |
| 1.1 | Emma Cooper, Kafico Ltd | Mar 19 – minor grammatical amendments |
| 1.2 | Hannah Calway, Kafico Ltd | Dec 19 – Amended protocol to widen scope from prescription collection to the collection of any PID by patients or their representative. |
| 1.2 | Emma Cooper, Kafico Ltd | Feb 20 – annual review – no amendments |
| 1.2 | Emma Cooper, Kafico Ltd | Feb 21 – annual review – no amendments |

Contents

[2. Scope 2](#_Toc37846066)

[3. Definitions 3](#_Toc37846067)

[4. Introduction 3](#_Toc37846068)

[5. Accountable Parties 3](#_Toc37846069)

[6. Context of Protocol 4](#_Toc37846070)

[7. Assessment Criteria 4](#_Toc37846071)

[8. Assessment 4](#_Toc37846072)

[Considered Scenarios 5](#_Toc37846073)

[The Patient has not authorised person to pick up information on their behalf 5](#_Toc37846074)

[Staff give out incorrect patient information 6](#_Toc37846075)

[9. Proposed Cluster Protocol – Prescriptions 7](#_Toc37846076)

[10. Proposed Cluster Protocol – All Other Information 7](#_Toc37846077)

[11. Associated Protocols 7](#_Toc37846078)

[12. Audit Schedule 8](#_Toc37846079)

[13. Review 8](#_Toc37846080)

# Scope

This policy has been drafted for use by customers of Kafico Ltd across Norfolk and Waveney.

At the time of writing and unless alternative policies have been adopted locally, the policy applies to;

|  |  |  |
| --- | --- | --- |
| Acle Medical Partnership | Boughton Doctors Surgery | Hellesdon Medical Practice |
| Beccles Medical Centre | Bridge Street Surgery | Holt Medical Practice |
| Birchwood Surgery | Cromer Group Practice | Feltwell Surgery |
| Blofield Surgery | St Clement's Surgery | Great Massingham and Docking Surgeries |
| The Brundall Medical Centre | Castle Partnership | The Harleston Medical Practice |
| Coltishall Medical Practice | The Burnhams Surgery | Heacham Group Practice |
| Campingland Surgery | Drayton Surgery | St John's Surgery |
| Hoveton & Wroxham Medical Centre | Roundwell Medical Centre | Staithe Surgery |
| Ludham Surgery | Paston Surgery | Thorpewood Surgery |
| The Market Surgery | Prospect Medical Practice | Upwell Health Centre and Welle Ltd |
| Howdale Surgery | Sheringham Medical Practice | Watlington Medical Centre |
| Litcham Health Centre | Southgate and Wootton’s | Wells Health Centre |
| Mundesley Medical Centre | St James Medical Practice | St Stephen’s Gate |
| Manor Farm Medical Centre | The Fakenham Medical Practice | Plowright Medical Centre |
| Grimston Medical Centre | Aldborough Surgery | Bacon Road / Taverham |
| The Burnham Surgery | Reepham & Alysham Surgery | Lakenham Surgery |
| Oak Street Medical Practice | UEA Medical Centre | Woodcock Road Surgery |
| Old Catton Medical Practice | Alexandra Road | Andaman Surgery |
| Attleborough Surgery | Beechcroft and Old Palace | Bridge Road |
| Bungay Medical Practice | Chet Valley Medical Practice | Church Hill Surgery |
| Cringleford Surgery | Cutlers Hill Surgery | East Harling Surgery |
| East Norfolk Medical Practice | Elmham Surgery | Falkland Surgery |
| Fleggburgh Surgery | Heathgate Medical Practice | Hemsby Medical Centre |
| High Street Surgery | Hingham Surgery | Hollies Surgery |
| Humbleyard Practice | Lawns Medical Practice | Lawson Road Surgery |
| Lighthouse Medical Centre | Lionwood Medical Practice | Long Stratton Medical Partnership |
| Longshore Surgery | Magdalen Medical Practice | Mattishall Surgery |
| Millwood Surgery | Old Mill Surgery | Orchard Surgery |
| Rosedale Surgery | School Lane Surgery | Shipdham Surgery |
| Solebay Health Centre | The Beaches Medical Centre | The Coastal Partnership |
| The Park Surgery | Theatre Royal Surgery | Toftwood Medical |
| Trinity Street Surgery | Victoria Road | Watton Medical Practice |
| West Pottergate Medical Practice | Windmill Surgery | Wymondham Medical Practice |

# 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.

# Introduction

This protocol intends to support practice staff and stakeholders in understanding the current protocol for patients or their representatives picking up any information requested from the practice. This could be a prescription for dispensing practices but also includes when a patient is picking up copies of their information.

# Accountable Parties

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 that information is processed in a fair and appropriate manner. 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.

# Context of Protocol

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 is balanced through a proportionate response that does not result in a significant increase in burden on the organisation.

# Assessment Criteria

In assessing the level of risk associated with unidentified individuals collecting prescriptions **The Practice** 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

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 pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by obligations of secrecy. | | 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 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 / papwerwork 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 protected by obligations of secrecy. | | 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 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. |

# Proposed Cluster Protocol – Prescriptions

1. Ask if collecting for themselves or another
2. Ask patients name, DOB & Address
3. View ID if not the patient
4. Get representative to print name & sign back of kept prescription form

# Proposed Cluster Protocol – All Other Information

1. Ask for patients’ name, DOB and address
2. Ask if they are the patient or picking up on behalf of the patient
3. If patients’ representative, ask to view ID and note the representative’s name.
4. Check name, DOB and address on information to be handed over.
5. Handover the information if it is the correct patient
6. Update relevant log to note who picked up the information.
   1. 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]

# Associated Protocols

This policy should be read in conjunction with;

* Risk Management Policy
* Change Management Policy
* Information Governance Policy
* Information Rights and Access Protocol
* Information Sharing and Privacy Protocol
* Information Lifecycle and Data Quality Protocol
* Information / Cyber Security Protocol
* Information Incident Protocol
* Data Protection Impact Assessment Protocol
* Freedom of Information Protocol

# Audit Schedule

Prescriptions should be audited twice a year to ensure they are being signed correctly.

# Review

This protocol will be reviewed every year or sooner where necessary.