Information Incident Protocol

|  |  |  |
| --- | --- | --- |
| Policy Title / Reference | Author | Owner |
| Information Incident Protocol | Emma Cooper, Cluster DPO (Kafico) | Practice Manager |

|  |  |  |
| --- | --- | --- |
| Version | Revision author | Version comments |
| 1 | Emma Cooper, Kafico Ltd (DPO) | Jan 18 New Draft |
| 1.1 | Emma Cooper, Kafico Ltd (DPO) | Jan 19 Replaced 1998 DPA with 2018 Act. Replaced GDPR with “data protection legislation”.Clarified that incidents must come through DPO.Inserted new incident form at appendix. Added information about the required contents of notification to affected individuals |
| 1.2 | Emma Cooper, Kafico Ltd (DPO) | Feb 19 Added information about how to respond when unauthorised access to personal data is discovered |
| 1.3 | Hannah Calway, Kafico Ltd (DPO) | Mar 19 Updated to Information Incident form to ensure streamline initial responses. |
| 1.4 | Hannah Calway, Kafico Ltd (DPO) | May 19 – updated to include hand over of investigation due to absence. |
| 1.5 | Hannah Calway. Kafico Ltd (DPO) | August 19 – Amendments to Incident form |
| 1.5 | Emma Cooper, Kafico Ltd (DPO) | Jan / Feb 20 – Annual review – no amendments |

Contents

[2. Scope 2](#_Toc37845330)

[3. Definitions 3](#_Toc37845331)

[4. Introduction 3](#_Toc37845332)

[5. Statutory Mandatory Framework 4](#_Toc37845333)

[6. Information Incident Reporting 4](#_Toc37845334)

[7. Unauthorized Access to Personal Data 5](#_Toc37845335)

[8. Incident Communication 5](#_Toc37845336)

[9. Handing Over Investigation – Annual Leave / Sickness / Days Off 6](#_Toc37845337)

[10. Accountable Parties 6](#_Toc37845338)

[11. What is an Information Incident? 6](#_Toc37845339)

[12. Associated Protocols 7](#_Toc37845340)

[13. Audit Schedule 7](#_Toc37845341)

[14. Review 7](#_Toc37845342)

[Appendix A: Information Incident Form 7](#_Toc37845343)

[Incident Details 7](#_Toc37845344)

[15. DPO Scoring Matrix 9](#_Toc37845345)

# Scope

This protocol has been drafted for use by customers of Kafico Ltd across Norfolk.

At the time of writing and unless alternative protocols have been adopted locally, the protocol 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 supports staff to deal with incidents involving Personal Confidential Information to ensure that they are appropriately controlled, reported and that lessons are effectively fed back into the risk management cycle.

# Statutory Mandatory Framework

It is essential that all Information Governance Serious Incidents Requiring Investigation (IG SIRIs) including IG Cyber SIRIS which occur in Health, Public Health and Adult Social Care services are reported appropriately and handled effectively.

All Organisations processing Health, Public Health and Adult Social Care Personal Confidential Information are required to use the IG Toolkit Incident Reporting Tool to report level 2 IG SIRIs to the DH, ICO and other regulators.

All Organisations processing Health, Public Health and Adult Social Care personal data are expected to use the IG Toolkit Cyber SIRI extended functionality to contribute to health and social response to the UK’s Cyber Security Strategy.

Level 2 Cyber Incidents will be notified to the Department of Health and NHS Digital / Information Commissioners Office.

# Information Incident Reporting

[insert practice name] is committed to compliance with the above requirements.

Where an incident of this type occurs, staff are required to complete an Incident Record Form (Appendix A) in the first instance.

This must be escalated to the DPO for review.

The IG Lead or Data Protection Officer will then investigate and grade the incident with in line with the NHS Digital Checklist[[1]](#footnote-2) and grade the incident.

Incidents must be reported as soon as possible (usually within 72 hours of a breach being notified/identified locally) and so it is important to contact the DPO as soon as possible with as much information as can be ascertained at the time.

All incident data, trends and lessons learned will be fed into the [insert practice name] Information Risk Management process and suitable mitigations implemented such as additional staff training or process improvement.

# Unauthorized Access to Personal Data

Where it is discovered that a staff member has accessed personal data inappropriately, for example accessing patients records without a genuine business need or accessing their own records or those of family, friends or colleagues without the permission of the organization. The information must be passed to the DPO immediately and a full audit performed of staff members’ access to clinical system and shared drives (where available).

This audit results must be passed to the DPO for review and staff member should be interviewed to determine the circumstances of the potentially inappropriate access. Staff members’ access should be limited or monitored whilst investigation is ongoing.

# Incident Communication

During investigation, the DPO will determine whether there needs to be communication with the affected data subjects based on whether the incident might 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 person concerned.

The following methods have been identified as possible approaches;

1 – 10 data subjects affected direct postal contact

10 – 50 data subjects affected direct email contact

50+ data subjects affected website alert, clinical system generated texts, in situ posters

This approach reflects that breaches affecting a greater volume of data subjects may cause concern amongst patient population or be difficult to arrange direct contact for. It is therefore necessary to ensure proactive communication and an opportunity for patients to ascertain if their information was involved and make enquiries or complaints.

* When notifying patients, the following information must be included;
* Name and contact details of DPO or other point of contact where more information can be obtained
* Nature of the breach and the contents of the information
* A description of measures taken / being taken to address the breach.
* A description of the likely consequences

# Handing Over Investigation – Annual Leave / Sickness / Days Off

When an incident arises the primary investigator within the organisation must ensure they document their investigation and findings in a shared space for those who have need to view and / or continue the investigation in the event of expected or unexpected absence. The ICO can issue fines for incidents reported outside of the legal 72 hour time frame unless they are satisfied with the reasons behind the delay. Furthermore, your DPO will be continuing the investigation and must be able to contact any member of staff for further details when necessary.

# 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 effective reporting and management of information risk for [insert practice name]. 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.

# What is an Information Incident?

Examples of types of information incidents include;

* Corruption or inability to recover electronic data
* Data disclosed in error
* Data lost in transit
* Lost or stolen hardware
* Lost or stolen paperwork
* Non-secure disposal – hardware or paperwork
* Technical security failing – including hacking
* Unauthorised access / disclosure
* Uploaded to website in error
* Data quality issue

# Associated Protocols

This protocol 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 Risk and Audit Protocol
* Data Protection Impact Assessment Protocol
* Freedom of Information Protocol

# Audit Schedule

Audits of this protocol will be fed into the Plan, Do, Check, Act cycle as referenced in the Information Risk and Audit Protocol.

# Review

This protocol will be reviewed every year or sooner where necessary

# Appendix A: Information Incident Form

NB: If you hover over the top left of the below table and click the cross that appears you can copy and paste the form into a new word document to fill in.

## Incident Details

|  |  |  |  |
| --- | --- | --- | --- |
| Date Incident Occurred: |  | Date Incident Discovered: |  |
| Time Of incident |  |
| Was the practice acting as a Processor on behalf of a Controller when the incident occurred? |  |
| Category (insert X) |  |
| Confidentiality: unauthorised or accidental disclosure of, or access to personal data |  |
| Availability: unauthorised or accidental loss of access to, or destruction of, personal data |  |
| Integrity: unauthorised or accidental alteration of personal data |  |
| Site of Incident |  |
| Location of Incident |  |
| Type of information disclosed:I.e. referral letter, prescription etc. Please include whether this is just DOB / Name or sensitive medial information as well. |  |
| Who was the information disclosed to? |  |
| Description of what happened: |  |
| Immediate Action Taken:Please include:Staff remindersActions to mitigate further disclosureIf the patient is aware of the incident. |  |
| Has the information disclosed been handed back to the practice? Or have you received written confirmation of destruction?If no, what steps are being taken to retrieve the information? |  |
| If completing investigation before alerting DPO – have you notified the patient of the incident? | If yes, please tick to confirm that each of the following information was provided:* Contact Details of DPO
* Nature of the breach and contents of the information
* Description of the measures taken / proposed to be taken
* Likelihood of consequences (including where you envisaged there to be none)
* You do have a right to make a complaint to us or the Information Commissioner, if you feel your request has not been managed appropriately. You can call them on 0303 123 1113 or write to them at;

Information Commissioner's OfficeWycliffe HouseWater LaneWilmslowCheshireSK9 5AFAdditionally, you also have a right to seek to enforce your rights through the courts. |
| ***TO BE COMPLETED BY DPO*** |
| Likelihood of adverse effect | *This will be completed by the Data Protection Officer* |
| Has there been or is there likely to be any media interest? |  |
| Who has been notified? |  |
| Trusted Partner? |  |
| Encryption? |  |
| Special categories/vulnerable groups? Min 4 impact |  |
| Conclusion: |  |

Please send to admin@kafico.co.uk

Once details have been provided to the Data Protection Officer, they will be loaded onto the NHS Digital Incident Reporting Tool in line with the provided guidance at https://www.dsptoolkit.nhs.uk/Help/29

# DPO Scoring Matrix

|  |  |
| --- | --- |
| Not occurred | There is absolute certainty that there can be no adverse effect. This may involve a reputable audit trail or forensic evidence |
| Not likely or any incident involving vulnerable groups even if no adverse effect occurred | In cases where there is no evidence that can prove that no adverse effect has occurred this must be selected. |
| Likely | It is likely that there will be an occurrence of an adverse effect arising from the breach. |
| Highly likely | There is almost certainty that at some point in the future an adverse effect will happen. |
| Occurred | There is a reported occurrence of an adverse effect arising from the breach. |

| No. | Effect | Description |
| --- | --- | --- |
| 1 | No adverse effect | There is absolute certainty that no adverse effect can arise from the breach |
| 2 | Potentially some minor adverse effect or any incident involving vulnerable groups even if no adverse effect occurred | A minor adverse effect must be selected where there is no absolute certainty. A minor adverse effect may be the cancellation of a procedure but does not involve any additional suffering. It may also include possible inconvenience to those who need the data to do their job. |
| 3 | Potentially some adverse effect | An adverse effect may be release of confidential information into the public domain leading to embarrassment or it prevents someone from doing their job such as a cancelled procedure that has the potential of prolonging suffering but does not lead to a decline in health. |
| 4 | Potentially Pain and suffering/ financial loss | There has been reported suffering and decline in health arising from the breach or there has been some financial detriment occurred. Loss of bank details leading to loss of funds. There is a loss of employment. |
| 5 | Death/ catastrophic event. | A person dies or suffers a catastrophic occurrence |



1. [↑](#footnote-ref-2)