Upwell Health Centre and Welle Ltd (Pharmacy)

Information Incident Protocol

|  |  |  |
| --- | --- | --- |
| Version | Author | Notes |
| 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 |
| 1.6 | Hannah Calway, Kafico Ltd (DPO) | Jun 20 – Updates to incident form |
| 1.7 | Hannah Calway, Kafico Ltd (DPO) | Dec 20 – Updates to incident form |
| 1.7 | Emma Cooper, Kafico Ltd (DPO) | Feb 21 - Annual Review – no amendments. |
| 1.7 | Emma Cooper, Kafico Ltd (DPO) | Mar 22 – annual review – no amendments. |
| 1.8 | Emma Kitcher, Kafico Ltd | Mar 23 – added an item under section 6 about ensuring incident trends are reported to senior organisation members.  Added items under Section around how the DPO supports with incidents. |

**Contents**

[1. INTRODUCTION 2](#_Toc129367526)

[2. QUICK REFERENCE POINTS 3](#_Toc129367527)

[3. KEY DEFINITIONS 3](#_Toc129367528)

[4. SCOPE 4](#_Toc129367529)

[5. KEY LEGISLATION / FRAMEWORK 4](#_Toc129367530)

[6. INFORMATION INCIDENT REPORTING 4](#_Toc129367531)

[7. UNAUTHORISED ACCESS TO PERSONAL DATA 5](#_Toc129367532)

[8. INCIDENT COMMUNICATION 5](#_Toc129367533)

[9. HANDING OVER INVESTIGATION – ANNUAL LEAVE / SICKNESS / ABSENCE 6](#_Toc129367534)

[10. REPORTING AN INCIDENT 6](#_Toc129367535)

[11. APPLICATION AND AUDIT 7](#_Toc129367536)

1. 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.

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.

1. QUICK REFERENCE POINTS

* Staff must be able to recognise an incident and promptly report it
* An incident is where the confidentiality, availability or integrity of personal data has been affected
* If you are investigating an incident, make sure you hand it to a colleague when you are absent
* Sometimes the patient will need to be notified
* Sometimes the authorities will need to be notified
* A timely response is important

1. 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.

1. 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 effective reporting and management of information incidents. 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.

1. KEY LEGISLATION / FRAMEWORK

* UK GDPR / Data Protection Act 2018
* Human Rights Act 1998

1. INFORMATION INCIDENT REPORTING

* Upwell Health Centre and Welle Ltd (Pharmacy) is committed to compliance with the above requirements.
* Where an incident of this type occurs, staff are required to complete an Incident Record Form ([Submit Incident Form](https://forms.office.com/pages/designpagev2.aspx?origin=NeoPortalPage&collectionid=kd327g80jcjf86swillfmk&subpage=design&id=Epvrg5Qa9UO0Lcg2kMrUjF8ZumccUwdJrZFK-zu_2xpUMFRLS0xTUFNJSFRESzIxMVBVUzY1QjlQWS4u)) or raise with the SIRO / Caldicott Guardian 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-1) 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 Upwell Health Centre and Welle Ltd (Pharmacy) Information Risk Management process and suitable mitigations implemented such as additional staff training or process improvement.
* Key incident trends and lessons will be escalated to the most senior members of the organisation.

1. UNAUTHORISED 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.

1. 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

1. HANDING OVER INVESTIGATION – ANNUAL LEAVE / SICKNESS / ABSENCE

* When an incident arises, the primary investigator within Upwell Health Centre and Welle Ltd (Pharmacy) 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, the Data Protection Officer (DPO) will be continuing the investigation and must be able to contact any member of staff for further details when necessary.

1. REPORTING AN 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

To report an incident to the DPO, please use the link at <https://forms.office.com/Pages/ResponsePage.aspx?id=Epvrg5Qa9UO0Lcg2kMrUjF8ZumccUwdJrZFK-zu_2xpUMFRLS0xTUFNJSFRESzIxMVBVUzY1QjlQWS4u>

* Once reported, the DPO will be in touch to obtain further information as required
* The DPO will advise of any immediate or longer-term mitigation steps to be taken
* Support will be provided in relation to making contact with affected data subjects
* A final incident report will be produced for practice records

1. 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.

* The organisation will list the information rights on our privacy policy
* All staff should be able to recognise and refer information rights requests to the right person
* All staff, visitors and service users should have access to the Data Protection Officer’s contact details to support with rights
* New projects, suppliers or systems must be raised with the Data Protection Officer for review
* The organisation will keep a log of all information rights requests to ensure that we are responding in a consistent and timely way
* 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
* Subject Access Requests are covered in the Disclosures and Access Protocol

1. [↑](#footnote-ref-1)