Upwell Health Centre and Welle Ltd (Pharmacy)

Information Risk and Change Management Protocol

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Author | Next Review Date | Notes |
| V1 (March 22) | Emma Kitcher, DPO | March 23 | New protocol that replaces IG06 (DPIA) and IG07 (Risk)Provides a more detailed description of a risk with some examplesDetails organisation’s PLAN, DO, CHECK, ACT approachIncludes DPIA checklist |
| V2 March 23 | Emma Kitcher, DPO | March 24 | Added an item under Section 10 (Data Protection Impact Assessments) about ensuring that the SIRO reviews any DPIAs and that recommendations and given due notice |

**Contents**

[INTRODUCTION 1](#_Toc97453786)

[QUICK REFERENCE POINTS 2](#_Toc97453787)

[KEY DEFINITIONS 2](#_Toc97453788)

[SCOPE 2](#_Toc97453789)

[KEY LEGISLATION / FRAMEWORK 3](#_Toc97453790)

[RISK MANAGEMENT 3](#_Toc97453791)

[PLAN 4](#_Toc97453792)

[DO 5](#_Toc97453793)

[CHECK / ACT 5](#_Toc97453794)

[DATA PROTECTION IMPACT ASSESSMENTS 7](#_Toc97453795)

[APPLICATION AND AUDIT 9](#_Toc97453796)

1. INTRODUCTION

This protocol intends to support the organisation and its staff in managing information risk to protect the organisation and its stakeholders from the inherent risks associated with processing Personal Confidential Information and managing change that affects information or systems.

Information Risk and Change Management are disciplines that support the organisation to operate within a complex framework of privacy legislation including Data Protection legislation, Common Law Duty of Confidence, Article 8 European Convention of Human Rights, Computer Misuse Act 1990 as well as health specific mandatory codes. Effective Information Risk Management protects the organisation and its stakeholders and allows for effective risk mitigation, planning and allocation of resources.

1. QUICK REFERENCE POINTS
* It is important that the organisation is able to identify information risk
* Risk can be present when things remain the same as well as well things change
* Certain tools such as registers, logs and assessments can support the organisation to manage information risk
* There are key roles involved – including the Data Protection Officer and Senior Information Risk Officer
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 risk. 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
* Caldicott Principles
* Human Rights Act 1998
1. RISK MANAGEMENT
* A risk is defined as a vulnerability combined with a threat.
* Some of these risks are ‘inherent’ which means that they exist, even if there is no change.

Example

There is a constant threat of cyber attack worldwide. Simply having and using computers that access the internet creates a vulnerability. This means there is always an inherent risk that our systems will be subject to cyber-attack. This will affect our ability to operate and could compromise the security of Personal Confidential Data.

* Some risks are a result of change. These ‘reactive’ risks can occur when new projects, systems or suppliers are engaged.

Example

The organisation is planning to engage a new HR system. There is a threat that the new provider is not of good standing and manages Personal Confidential Information poorly. The nature of HR information (sensitive information about employees work and home lives) creates a vulnerability. There is a risk that the new HR system does not protect the Personal Confidential Information of employees, and this will result in harm to individuals and the reputation of the organisation.

* The organisation‘s Information Risk Management takes the form of a Plan, Do, Check, Act cycle as demonstrated in the diagram below.



* This can be applied to both inherent and reactive risks.
* All audit, review and incident outcomes are fed into senior management where recommendations are made as to how controls can be applied or improved for greater assurance.
1. PLAN
* The following items form the basis for the Upwell Health Centre and Welle Ltd (Pharmacy) information risk management plan;
* The organisation will put in place an Information Risk Register which is managed by the Senior Information Risk Officer
* A suitably knowledgeable Data Protection Officer has been appointed
* Policies and protocols are produced as a plan to manage both inherent and reactive risks
* A Processing Activities Log is in place to provide a baseline for activities that use Personal Confidential Information
1. DO
* The following items demonstrate how the Upwell Health Centre and Welle Ltd (Pharmacy) information risk management plan will be implemented.
* The Information Risk Register will be regularly reviewed and updated, and key items will be escalated to the most senior members of the organisation by the Senior Information Risk Manager (SIRO)
* The Data Protection Officer (DPO) will ensure that staff are trained and supported regarding data protection compliance
* The DPO will highlight risks to the SIRO via regular updates, newsletters or meetings
* Data Protection Impact Assessments will be completed by the DPO and reviewed by the SIRO
* Key learning will be shared following information incidents and measures put in place to prevent recurrence
* A Processing Activities Log will be reviewed / submitted by the organisation twice a year
* New projects, providers and systems will be notified to the DPO for review
* The SIRO and DPO will be suitably trained to ensure that they can fulfil their responsibilities
1. CHECK / ACT
* The following items demonstrate how the Upwell Health Centre and Welle Ltd (Pharmacy) information risk management plan will be checked.
	+ The Senior Information Risk Officer (SIRO) will ensure that data protection and security policies and protocols are up to date and have been circulated to all staff, including new starters
	+ The organisation will submit an NHS Data Protection and Security Toolkit each year as a self-assessment. It provides an opportunity to reflect on the information risk management plan.
	+ Data Protection Impact Assessments will be revisited by the DPO after 12 months to ensure that the identified risks are still being mitigated.
	+ The DPO will make a Compliance Spot Check template available or organise an audit to provide a view on risk across the organisation
	+ The SIRO will ensure that audits of how, when and why people are accessing systems are happening regularly for high risk systems such as clinical or HR systems
	+ System Administrators will be allocated to key systems to monitor risk associated with those systems such as shared logins or poor quality data
	+ Incident trends will be monitored by the DPO and SIRO to ensure that mitigations are being put in place prior to significant events occurring
	+ The DPO will undertake due diligence on new providers that includes
		- Checking ICO registration
		- Checking for data breaches
		- Checking international transfers
		- Reviewing for lawful contracts against UK GDPR Art 28
	+ The DPO will undertake due diligence on new systems that includes
		- Checking the system provider as above
		- Checking security measures
	+ Providers or systems that do not pass due diligence will be notified to the SIRO by the DPO
	+ If there are signs that staff are not understanding or following policy or protocol, the SIRO will escalate to the DPO for amendment
	+ The SIRO and DPO will be renew their training regularly to ensure that they can fulfil their responsibilities
1. DATA PROTECTION IMPACT ASSESSMENTS
* The process of completing a DPIA can be complex and require specialist skills and so will usually be completed by the Data Protection Officer.
* This section acts as a precursor to a full DPIA and allows the organisation to determine whether the change being considered warrants a full DPIA and gives an indication of the types of risks involved and mitigations to be put in place.
* A Data Protection Impact Assessment (DPIA for short) is used as a living document that ensures any new process being considered that is likely to result in a high risk to the rights of data subjects has gone through a thorough screening that aids in mitigating risks and weighing the risks against the outcome.
* There are different times when a DPIA is needed. The ICO has issued guidance on this. The table will be used by the DPO as an initial determination of whether a DPIA is needed. If the answers are inconclusive, an initial DPIA should be conducted to make a determination
* A DPIA must start **before** the processing begins to ensure there is a legitimate gateway to be able to process the data.
* Send all new projects or changes to the DPO to be reviewed.
* The DPO **must** be involved in the DPIA and even once the project is up and running the DPIA should sit beside it and update as the project updates to ensure continuous compliance with the data protection legislation and ICO guidance.
* DPIAs approved by the DPO should be shared with the SIRO. Any recommendations should be noted and built into processes.

The grids below will be used to determine whether a DPIA is required in each instance.

|  |
| --- |
| If you tick **any** of the sections below, the DPO should ***consider*** a DPIA. |
| Evaluation or scoring |  |
| Automated decision-making with significant effects |  |
| Systematic monitoring |  |
| Processing of sensitive data or data of a highly personal nature |  |
| Processing on a large scale |  |
| Processing of data concerning vulnerable data subjects |  |
| Innovative technological or organisational solutions |  |
| Processing that involves preventing data subjects from exercising a right or using a service or contract |  |

|  |
| --- |
| If you tick **any** of the sections below, the project **requires** a DPIA. |
| Systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person |  |
| Processing on a large scale of special categories of data or of personal data relating to criminal convictions and offences |  |
| Systematic monitoring of a publicly accessible area on a large scale |  |
| Use profiling, automated decision-making or special category data to help make decisions on someone’s access to a service, opportunity or benefit |  |
| Combine, compare or match data from multiple sources |  |
| Process children’s personal data for profiling or automated decision-making or for marketing purposes, or offer online services directly to them |  |
| Process personal data that could result in a risk of physical harm in the event of a security breach |  |

|  |
| --- |
| If you tick **TWO** of the sections below, the project **requires** a DPIA. |
| Processing biometric or genetic data[[1]](#footnote-1)  |  |
| Use of innovative technology[[2]](#footnote-2) |  |
| Processing personal data without providing a privacy notice directly to the individual  |  |
| Processing personal data in a way that involves tracking individuals’ online or offline location or behaviour |  |

* If threshold is met, the DPO will complete a DPIA that includes;
* Data Flow Map
* Controllers and Processors
* Lawful Basis
* Transparency
* Information Rights
* Technical and Organisation Measures to Protect Personal Data
1. APPLICATION AND AUDIT
* 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
1. DNA, facial images, fingerprints, tissue samples [↑](#footnote-ref-1)
2. Artificial intelligence, machine learning and deep learning; connected and autonomous vehicles; intelligent transport systems; smart technologies (including wearables); market research involving neuro-measurement (e.g. emotional response analysis and brain activity); some ‘internet of things’ applications, depending on the specific circumstances of the processing. [↑](#footnote-ref-2)