



Information Governance

Data Protection and Confidentiality Policy

Policy Title	Data Protection and Confidentiality Policy
Author/Contact	Holly Hellstrom - Information Assurance Director Calum Hall - Data Protection Officer
Document Reference	OH/IG/IGMF
Version	2
Status	Approved
Publication Date	April 2024
Review Date	January 2025
Approved by	Jeremy Fowler - SIRO Dr James Britton - Caldicott Guardian
Ratified by	Information Governance Team

Version	Date	Comments	Author	Notes
1	16/12/2022	Approved by IGT	Information Assurance Director	Amalgamation of CP and WHN. UKGDPR
2	8/4/2024	Approved by IGT	Data Protection Officer	Updated to reflect NHS DSP guidelines

Contents

Background.....	3
Statement	3
Introduction	3
Purpose.....	3
Principles	4
Underpinning policies and procedures	5
Data protection by design and by default.....	5
Responsibilities	6

Background

Ozone Health Ltd is the overarching board and governance for Ozone Health Ltd (OH), Clinical Partnership (CP) & The World Healthnet Ltd (WHN). The Ozone Health Group aims to ensure that all the Healthcare and Healthcare IT services it provides, commissions, contracts for and maintains are of the highest quality and good customer care is at the heart of the group's success.

The Group is required to meet its legal obligations and NHS requirements concerning confidentiality and information security standards.

The requirements within the Policy are primarily based upon the Data Protection incorporating the UK General Data Protection Regulation and the Data Protection Act 2018, which is the key piece of legislation covering security and confidentiality of Personally Identifiable Data (PID).

Statement

This policy covers records held and processed by the Group, which is responsible for its own records under the terms of the Act and it has submitted a notification as a Controller to the Information Commissioner.

This Policy will apply to:

- All staff including any temporary staff, sub-contractors & contractors
- Information or systems used and managed by the Group
- Any individual using or requires access to information 'owned' by the Group

Introduction

The Group has a legal obligation to comply with all appropriate legislation in respect of data, information and data security. It also has a duty to comply with guidance issued by the Department of Health and Social Care (DHSC), the Information Commissioner Office (ICO), other advisory groups to the NHS and guidance issued by professional bodies.

Penalties could be imposed upon the Group and/or employees for non-compliance with relevant legislation and NHS guidance.

This Data Protection Policy is the overarching policy for data security and protection for Ozone Health Ltd. (hereafter referred to as "us", "we", or "our").

Purpose

The purpose of the Data Protection Policy is to support the 10 Data Security Standards, the General Data Protection Regulation (2016), the Data Protection Act (2018), the common law duty of confidentiality and all other relevant national legislation. We recognise data protection as a fundamental right and embrace the principles of data protection by design and by default.

This policy covers:

- Our data protection principles and commitment to common law and legislative compliance
- Procedures for data protection by design and by default.

Principles

We will be open and transparent with service users and those who lawfully act on their behalf in relation to their care and treatment. We will adhere to our duty of candour responsibilities as outlined in the Health and Social Care Act 2012.

We will establish and maintain policies to ensure compliance with the Data Protection Act 2018, Human Rights Act 1998, the common law duty of confidentiality, the General Data Protection Regulation and all other relevant legislation.

We will establish and maintain policies for the controlled and appropriate sharing of service user and staff information with other agencies, taking account all relevant legislation and citizen consent.

Where consent is required for the processing of personal data we will ensure that informed and explicit consent will be obtained and documented in clear, accessible language and in an appropriate format. The individual can withdraw consent at any time through processes which have been explained to them and which are outlined in the NHS National Opt-Out Policy. We ensure that it is as easy to withdraw as to give consent.

We will undertake annual audits of our compliance with legal requirements.

We acknowledge our accountability in ensuring that personal data shall be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')
- Accurate and kept up to date
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed ('storage limitation')
- Processed in a manner that ensures appropriate security of the personal data.

We uphold the personal data rights outlined in the GDPR:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling.

In line with legislation, we employ a Data Protection Officer (DPO) who will report to the highest management level of the organisation. We will support the DPO with the necessary resources to carry out their tasks and ensure that they can maintain expertise. We guarantee that the

DPO will not be pressured on how to carry out their tasks, and that they are protected from disciplinary action when carrying out the tasks associated with their role.

We complete the Data Security and Protection Toolkit on an annual basis and our publication status can be found here: <https://www.dsptoolkit.nhs.uk/OrganisationSearch/M0V3X>

Underpinning policies and procedures

This policy is underpinned by the following:

- Quality Management Policy – outlines procedures to ensure the accuracy of records and the correction of errors
- Record Management & Lifecycle Policy – details transparency procedures, the management of records from creation to disposal (inclusive of retention and disposal procedures), information handling procedures, procedures for subject access requests, right to erasure, right to restrict processing, right to object, and withdrawal of consent to share
- Data Security & Confidentiality Policy – outlines procedures for the ensuring the security of data including the reporting of any data security breach
- Business Continuity Procedure – outlines the procedures in the event of a security failure or disaster affecting digital systems or mass loss of hardcopy information necessary to the day to day running of our organisation
- Staff Confidentiality Clause (in contract) - provides staff with clear guidance on the disclosure of personal information.

Data protection by design and by default

We shall implement appropriate organisational and technical measures to uphold the principles outlined above. We will integrate necessary safeguards to any data processing to meet regulatory requirements and to protect individual's data rights. This implementation will consider the nature, scope, purpose and context of any processing and the risks to the rights and freedoms of individuals caused by the processing.

We shall uphold the principles of data protection by design and by default from the beginning of any data processing and during the planning and implementation of any new data process.

Prior to starting any new data processing, we will assess whether we should complete a Data Protection Impact Assessment (DPIA) using the ICO's screening checklist.

All new systems used for data processing will have data protection built in from the beginning of the system change.

All existing data processing has been recorded on our DPIA Register. Each process has been risk assessed and is reviewed annually.

We ensure that, by default, personal data is only processed when necessary for specific purposes and that individuals are therefore protected against privacy risks.

In all processing of personal data, we use the least amount of identifiable data necessary to complete the work it is required for and we only keep the information for as long as it is required for the purposes of processing or any other legal requirement to retain it.

Where possible, we will use pseudonymised data to protect the privacy and confidentiality of our staff and those we support.

Responsibilities

Our designated Data Security and Protection Lead is Calum Hall. The key responsibilities of the lead are:

- To ensure the rights of individuals in terms of their personal data are upheld in all instances and that data collection, sharing and storage is in line with the Caldicott Principles
- To define our data protection policy and procedures and all related policies, procedures and processes and to ensure that sufficient resources are provided to support the policy requirements
- To complete the Data Security & Protection Toolkit (DSPT) annually and to maintain compliance with the DSPT
- To monitor information handling to ensure compliance with law, guidance and the organisation's procedures and liaising with senior management and DPO to fulfil this work

Our designated DPO is Calum Hall, they can be contacted via email: calum@ozonehealth.co.uk; phone: 0333 577 6166; or at the following address: Pod 2, The Treetops, Hesslewood Hall Business Centre, Ferriby Road, Hessle, HU13 0LH.

The key responsibilities of the DPO are:

- Overseeing changes to systems and processes
- Monitoring compliance with the GDPR and the Data Protection Act 2018
- Completing DPIA
- Reporting on data protection and compliance with legislation to senior management
- Liaising, if required, with the Information Commissioner's Office (ICO).

Title of Service/Policy	Data Protection and Confidentiality Policy
Is this a new or existing service/policy?	Existing

1. Would this service or policy be aimed at any particular equality group?			
	Yes	No	If yes...
Age	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
Disability	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
Gender Identity (transgender)	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
Marriage and Civil Partnership	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
Pregnancy and Maternity	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
Race	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
Religion and Belief	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
Sex (Gender)	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
Sexual Orientation	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
Social Exclusion	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
Economic	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
Deprivation	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
Rural Isolation	<input type="checkbox"/>	<input checked="" type="checkbox"/>	

2. Would the service/policy potentially exclude or have a negative impact on any of the equality groups?			
	Yes	No	If yes...
Age	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
Disability	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
Gender Identity (transgender)	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
Marriage and Civil Partnership	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
Pregnancy and Maternity	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
Race	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
Religion and Belief	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
Sex (Gender)	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
Sexual Orientation	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
Social Exclusion	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
Economic	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
Deprivation	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
Rural Isolation	<input type="checkbox"/>	<input checked="" type="checkbox"/>	


3. Are there any known barriers which would obstruct access to this service/pathway?

	Yes	No	Barriers can include physical, geographical, communication, etc.
Age	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
Disability	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
Gender Identity (transgender)	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
Marriage and Civil Partnership	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
Pregnancy and Maternity	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
Race	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
Religion and Belief	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
Sex (Gender)	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
Sexual Orientation	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
Social Exclusion	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
Economic	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
Deprivation	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
Rural Isolation	<input type="checkbox"/>	<input checked="" type="checkbox"/>	

4. What evidence has been used to assist you to make the judgements in questions 1-3?

Demographic data and other status including census findings	<input type="checkbox"/>
Result of research findings including studies of deprivation	<input type="checkbox"/>
Results of recent consultations and surveys	<input type="checkbox"/>
Results of ethnic monitoring data and any equalities data from Local Authority/Public Health etc.	<input type="checkbox"/>
Information from other agencies or groups	<input checked="" type="checkbox"/>
Comparisons between similar policies/ services	<input type="checkbox"/>
Analysis of patient and public involvement	<input type="checkbox"/>
Analysis of audit reports and reviews	<input type="checkbox"/>
Community engagement and consultation events	<input type="checkbox"/>
CHECKLIST FOR BOARD SIGN OFF	
Please complete all the below relevant tick boxes	

	Yes	No	Comments
By completing and submitting this EIA we agree to all contents being published on the group website.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
By signing this EIA we confirm that we have made all the necessary enquiries in relation to this service and in good faith that relevant steps and plans are in place to mitigate any potential discrimination in the service we provide.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
We understand that if we identify an action this is absolutely fine and demonstrates that we are willing to review our service and tailor it to the needs of the community.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
We understand that progress on any identified actions will be discussed at the contract review meetings. If required we will ensure that all action plans are available for review at these meetings.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
We understand that this EIA relates to a particular service. Our Equality and Diversity policy may also be requested in order for us to demonstrate our commitment to equality legislation.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
We are aware of the new Equality Act 2010 and are committed to ensuring that all our policies and procedures reflect the legislation. Full details can be found at:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	

Date of Screening	March 2024
Risk Identified in EIA	None
Review Date	January 2025
Title of Person Conducting the Review	Information Assurance Director
Signature	
Full Assessment Review Date	N/A
Board Sign Off Date and Committee	IGT – 8/4/2024