Information Governance

Data Protection & Confidentiality Policy

Policy Reference: OHCPWHN/IG/DPC V1

Policy Title		Data Protection Confidentiality Policy		
Author/Contact		Holly Hellstrom – Information Assurance Director		
Document Ref		CP/IG/IGMF		
Version		1		
Status		Approved		
Publication Date		December 2022		
Review Date		January 2025		
Approved by		Mr J Fowler - SIRO & Dr James Britton – Caldicott Guardian		16/12/2022
Ratified by		Information Governance Team		16/12/2022
Version	**Date**	**Comments**	**Author**	**Notes**
1	16/12/2022	Approved by IGT	Information Assurance Director	Amalgamation of CP and WHN. UKGDPR

Contents

- Background
- Statement
- Introduction
- Aim
- Legislation
- Roles & Responsibilities
- Security & Confidentiality
- Disclosure of Information & Information in Transit
- Training
- Contracts of Employment/Contracting
- Disciplinary
- Data Subject Access Request (DSAR)
- Data Subject Rights
- Disclosure of Personal Information
- Save Haven and Information Sharing
- Monitoring
- Relevant Policies and Procedures

Background

Ozone Health Ltd is the overarching board and governance for Ozone Health Ltd (OHL), Clinical Partnership (CP) & The World Healthnet Ltd (WHN). 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.

Aim

This Group will meet its legal obligations and NHS requirements concerning confidentiality and information security standards. The requirements are based on the Data Protection (DP) legislation as this is the key piece of legislation covering security and confidentiality of PID.

Legislation

For the purpose of this Policy other relevant legislation may be referenced.

- Data Protection Act 2018 and UK GDPR
- Access to Health Records Act 1990
- Human Rights Act 1998
- Freedom of Information Act 2000

The following are the main publications referring to security and confidentiality of PID:

- Confidentiality: NHS Code of Practice
- Records Management Code of Practice 2021
- Employee Code of Practice (Information Commissioner)
- National Data Guardian for Health and Care Review of Data Security, Consent and Opt- Outs

Roles & Responsibilities

All staff are responsible for any records or data they create and with information they use.

Caldicott Guardian (CG)

Responsibility for safeguarding the confidentiality of patient information and enabling appropriate information-sharing.

Data Protection Officer (DPO)

To ensure the processing of personal data is in compliance with the applicable UK Data Protection Regulation and act as a contact point for data subjects and the Information Commissioner's Office (ICO).

Digital/IT Group (DIG)

The DIG are responsible for coordinating improvements in data protection, confidentiality, information security and cyber security and over-seeing integrated Group policies and reviewing procedures and risk issues and raising IG concerns to the Group's Board.

Managers

Directors and senior managers are responsible for ensuring that all staff comply with the policies and procedures and staff attend training on an annual basis, implement any necessary and reasonable changes required and ensure that any PID held is up to date and accurate.

All Staff

All staff, whether permanent, temporary or contracted are responsible for ensuring they are aware of the requirements incumbent upon them and for ensuring they comply with these on a day-to-day basis.

Security & Confidentiality

All information relating to identifiable data and any information that may be deemed sensitive, must be kept secure at all times. The Group shall ensure there are adequate policies and procedures in place to protect against unauthorised processing of information and against accidental loss, destruction and damage to the information.

Disclosure of Information & Information in Transit

It is important that information about identifiable individuals should only be disclosed on a strict legitimate 'need to know basis'.

Some disclosures may occur because there is a statutory requirement to disclose e.g. with a Court Order because other legislation requires disclosure under UK GDPR.

Portable media such as: disc, USB memory stick should be encrypted, or manual paper records scanned and sent by secure-mail or encrypted envelope. (Please see Sending and Transferring Data Securely policy)

If a member of staff wishes to process PID outside of the United Kingdom, the DPO must be consulted prior to any agreement to transfer or process information.

Training

This is carried out through formal awareness and training facilitated via the Groups Induction and Mandatory Annual Training updates.

Training on Data Confidentiality, Security and Compliance requirements under the Data Protection legislation shall be included in the staff induction process
An ongoing awareness programme shall be maintained to ensure that staff awareness is refreshed and updated as necessary

All staff will be made aware of what could be classed as a Data Security Breach and the process to follow so that incidents can be identified, reported, monitored and investigated.

Contracts of Employment/Contracting

Staff contracts of employment are produced and monitored by the Human Resources Team.

Staff security requirements shall be addressed at the recruitment stage and all contracts of employment shall contain a confidentiality clause.

Contractors and Sub-contractors' security requirements shall be addressed at the onboarding and compliance stage and all contracts shall contain a confidentiality clause.

Disciplinary

A breach of the DP principles could result in a member of staff facing disciplinary action. A copy of the Disciplinary Policy is available on the Groups HRFile sharepoint.

Data Subject Access Request (DSAR)

Legislation allows an individual (Data Subject) a right of access to data processed by the Group and is obliged to respond within one complete month. An extension of a further sixty days may be applied in exceptional circumstances where the request is likely to take longer than the statutory timescale. The Group will inform the requester explaining the delay and agree a new deadline.

Failure to do so is a breach of the legislation and could lead to a complaint to the ICO.

Data Subject Rights

Under the UK GDPR, data subjects have enhanced rights. These include:

- 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.

Disclosure of Personal Information

There are Acts of Parliament that govern the disclosure of personal information. Some of these Acts make it a legal requirement to disclose and others that state that information cannot be disclosed.

In the event a request for disclosure is made referencing any of these Acts the DPO may require notification prior to any information release.

Professional bodies (e.g. NMC, GMC, CIPFA, CIMA) often release guidelines and advice for their own disciplines. These guidelines should not conflict with this policy or legislative requirements.

Save Haven and Information Sharing

All NHS organisations and providers require haven procedures to maintain the privacy and confidentiality of the PID held. The implementation of these procedures facilitates compliance with the legal requirements placed upon the Group.

Where departments within the Group, NHS and/or other agencies want to send PID to a Group department, they should be confident that they are being sent to a location which ensures the security of the data.

Several Acts and guidance dictate the need for 'Safe Haven' arrangements, they include:

Confidentiality: NHS Code of Practice: Annex A1 Protect Patient Information *"Care must be taken, particularly with confidential clinical information, to ensure that the means of transferring from one location to another are secure as they can be"*

Scope

This provides:

- The legislation and guidance which dictates the need for a safe haven
- When a Safe Haven is required and requirements and procedures to implement
- Rules for different kinds of safe haven

The processes described in this policy must be followed by all Group staff, unless exceptional circumstances arise, which may have an impact on direct patient care.

This may include formal action in line with the Disciplinary process for Group employees; and other action in relation to other workers, which may result in the termination of an assignment, placement, secondment or honorary arrangement. Non-compliance may also lead to criminal action being taken.

Safe Haven

The term is a location where arrangements and procedures are in place to ensure PID can be held, received and communicated securely.

However, any department sending, receiving, holding or communicating PID, should provide safe haven conditions by following the guidelines set out within this policy.

Personally Identifiable Data (PID)
PID is any data that can be used to clearly identify an individual and **GDPR** also references sensitive personal data.

Special Category Data
Personal data revealing **racial or ethnic origin**; **political opinions**, **religious or philosophical beliefs, trade union membership**; **genetic data**; **biometric data** (where used for identification purposes, **data concerning health**, **a person's sex life; and sexual orientation**.

Data Flow Mapping
This is the process of documenting the flow of information from one physical location to another and the method by which it "flows". Data flows may be by: E mail, post/courier, text or portable electronic or removable media.

Anonymised Information
Anonymised data is data that is has been rendered unidentifiable in such a way that the natural person cannot be identified from that data.

Data Sharing Agreements
The document sets out the general reasons and principles for information sharing. It shows that all signatory agencies are committed to maintaining agreed standards on handling information.

Safe Havens - Location/Security Arrangements

- Consideration should be given to the physical security arrangements i.e. locked room or accessible via a keycode, only known to authorised staff, or swipe card controlled. In particular at Head Office where hotdesking takes place.
- The office or workspace area should only be accessible to authorised members of staff in the same building.
- Windows should have locks and the room should conform to health and safety requirements in terms of fire, safety from flood, theft or environmental damage.
- Paper records containing PID must be stored in locked cabinets / rooms, where possible.
- Digital information should not be left on view or accessible to unauthorised staff and the screen 'locked' or logged/switched off when not in use.

Fax Machines
Information should not be faxed as per 2020 regulations. Faxing must only be used in emergencies and agreement from the Information Governance Team.

These must only be used for Business Continuity Planning (BCP) where it is **necessary**; e.g. Major Incident or Pandemic when the infrastructure to use other secure means of communication is affected.

Communication by Post
Transit envelopes must not be used for when PID is sent.

- All confidential information must be placed face down and not left unsupervised
- Mail should be opened away from public areas
- Outgoing post should be securely sealed in robust envelopes and clearly addressed to the department address or addressee only.

- Paper Records can be scanned and sent electronically by secure e-mail or using encryption Tools available.

Information should be stored on the Group's network and **not** on local computer hard drives i.e. 'C' drive (usually 'my documents') due to potential failure.

- PID and Commercially Sensitive must be stored securely and restricted as appropriate.
- Regular housekeeping of files to ensure only the minimum amount is retained.
- Any new system / project / change in data flow must undertake a Data Protection Impact Assessment (DPIA) and registered as an Information Asset to comply with DP legislation, Caldicott principles and DSPT requirements.

Phone

- Information should not usually be provided over the telephone unless the identity of the caller can be verified
- Confirm the reason for the information request, take a contact number or switchboard, check whether the information can be provided; if in doubt, call the enquirer back and provide to the person requesting it

Transportation Arrangements

- PID should only be taken off site when absolutely necessary and transported in a sealed container (where possible). Please refer to the Sending and Transferring Information Securely Policy.
- Never leave unattended and ensure all information is returned back to site as soon as possible, and records are updated

Displaying Personal Information (for example on white-boards)

Boards must be sited in areas that are **not** accessible by the public, e.g. staff offices. These rooms should be clearly marked 'staff only' and windows obscured appropriately.

If it is absolutely necessary to put information onto a whiteboard, it should be abbreviated or symbolised so only health professionals or staff can understand it. These areas should be carefully considered with a risk assessment undertaken by an appropriate manager.

Sharing Information with other Organisations

- You have consent or
- If a law says you have to or
- It's in the public interest
- Direct Care purposes
- Department for Health and Social Care in response to a Pandemic

The Group must be assured that organisations are able to comply with the safe haven ethos and meet certain legislative and related guidance requirements:

- DP legislation
- Common Law Duty of Confidentiality
- Confidentiality: NHS Code of Practice

Data sharing agreements must be put in place where personal information is to be shared. All flows of information in and going out of the department should be risk assessed as appropriate.

Monitoring

The Group will undertake or commission assessments and audits of its framework, policies and procedures to monitor compliance and make improvements where identified.

This policy will be reviewed every two years, and in accordance with the following on an as and when required basis if the following occurs:

- Legislative changes;
- good practice;
- guidance; case law;
- significant incidents reported;
- new vulnerabilities; and
- changes to organisational infrastructure.

Where there are no significant alterations required, this Policy shall remain for a period of no longer than two years of the ratification date.

Relevant Policies and Procedures

The following policies and procedures should be read in conjunction with this policy:

- Information Governance Policy;
- Staff Policies
- Sending & Transferring Information Securely
- Subject Access Request Policy

Title of Service/Policy Data Protection & Confidentiality Policy
Is this a new or existing Policy/service? New

1. Would this service or policy be aimed at any particular equality group?			
	Yes	No	If yes……
Age	☐	☒	
Disability	☐	☒	
Gender Identity (transgender)	☐	☒	
Marriage and Civil Partnership	☐	☒	
Pregnancy and Maternity	☐	☒	
Race	☐	☒	
Religion and Belief	☐	☒	
Sex (Gender)	☐	☒	
Sexual Orientation	☐	☒	
Social Exclusion	☐	☒	
Economic Deprivation.	☐	☒	
Rural Isolation	☐	☒	
Social Stigma	☐	☒	

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

3. Are there any known barriers which would obstruct access to this service/pathway			
	Yes	No	Barriers can include physical, geographical, communication.
Age	☐	☒	
Disability	☐	☒	
Gender Identity (transgender)	☐	☒	
Marriage and Civil Partnership	☐	☒	
Pregnancy and Maternity	☐	☒	
Race	☐	☒	
Religion and Belief	☐	☒	
Sex (Gender)	☐	☒	
Sexual Orientation	☐	☒	
Social Exclusion	☐	☒	
Economic Deprivation.	☐	☒	
Rural Isolation	☐	☒	
Social Stigma	☐	☒	

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.	☐	
Result of research findings including studies of deprivation.	☐	
Results of recent consultations and surveys.	☐	
Results of ethnic monitoring data and any equalities data from Local Authority/Public Health etc.	☐	
Information from other agencies or group	☐	
Comparisons between similar policies/services	☒	
Analysis of Patient and Public Involvement	☐	
Analysis of audit reports and review.	☐	
Community Engagement and consultation events.	☐	
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.	☒	☐	
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.	☒	☐	
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.	☒	☐	
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.	☒	☐	
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.	☒	☐	
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:	☒	☐	

Date of Screening	December 2022
Risk identified in EIA	None
Review Date	January 2025
Title of person conducting the review	Information Assurance Director
Signature	Holly Hellstrom
Full Assessment Review Date	N/a
Board sign off Date and Committee	IGT – December 2022