Workforce Repository and Planning Tool

Information Governance Pack

CONTENTS

Purpose

WRaPT is the ***Workforce Repository and Planning Tool*** which enables the collection, analysis and modelling of workforce information from organisations and providers across the whole health and social care economy. It is a flexible tool which at its core establishes the relationship between workforce capacity and service activity.

It has been designed to provide a secure workforce repository and reporting function and facilitates the ***analysis*** of large amounts of workforce and activity data across multiple organisations, creating the ability to align workforce with activity without utilising personally identifiable data. Scenarios can be ***modelled*** on any number of future states based on workforce, activity and efficiency changes. WRaPT does not seek to replicate financial modelling, safer staffing or eRostering tools, nor does it replace service knowledge, creative thinking and expertise. Rather, the use of WRaPT promotes ***meaningful discussions*** between teams, organisations and cross economy groups.

The purpose of this document is to detail the standards, policies and protocols employed by the WRaPT Team to ensure all processing is carried out fairly and in accordance with all relevant legislation.

WRaPT Information Governance Contracting Arrangements

The WRaPT Tool and service has been commissioned by Health Education England (North West) and is hosted by Lancashire Care NHS Foundation Trust. It is delivered in partnership between Lancashire Care NHS Foundation Trust and GE Healthcare Finnamore. The tool was developed initially in-house through NHS IT experts and then put out to a small developer when the size and scale of the tool significantly expanded. Robust contracting arrangements are in place between all the partners involved in the commissioning, development, hosting and delivery of WRaPT outlining the responsibilities of those organisations in respect of information governance and any relevant legal or organisational policies and procedures.

Data Protection Act (DPA)

The WRaPT Team take their responsibilities under the DPA very seriously. As a service we review and reflect on our policies and procedures to ensure that we operate within relevant legislation and organisational requirements. The Team IG Lead is responsible for reviewing the DPA and informing the WRaPT Service and Team in terms of any relevant changes to operating procedures.

Data in WRaPT could be identifiable, this is because whilst the only personally identifiable record (Employee Number) is pseudonymised, it is possible to identify an individual within a small team using individual characteristics such as gender and age. It is also sensitive, because it could include protected characteristics such as sexuality and race. As a result, the WRaPT team has developed its own procedures aligned with those of the host organisation, Lancashire Care NHS Foundation Trust.

Compliance with Data Protection Act (especially fair processing)

There are 8 data protection principles:

Specifically for WRaPT, these principles mean:

1 – ***Fairly and lawfully processed***. Specifically, this principle states:

- Do not use the data in ways that have unjustified adverse effects on the individuals concerned – in all cases WRaPT is about making informed decisions, including not adversely affecting any one group.
- Be transparent about how you intend to use the data, and give individuals appropriate privacy notices when collecting their personal data – staff know the data is being collected in the organisation itself - we ask organisations to include a statement for using the information across an economy, and ensure that appropriate data sharing is in place, signed off by the SIRO or Caldicott Guardian.

- Handle people's personal data only in ways they would reasonably expect – we put in place security as set out below.
- Make sure you do not do anything unlawful with the data – all WRaPT users are bound by the Data Protection Act as well as their own internal IG regulations.

2 – ***Processed for limited purposes***: Data is used for:

- Repository – providing a secure storage facility for workforce and activity data to be used for workforce planning purposes
- Workforce baseline – providing a view on the workforce across a Health & Social Care System. Use of protected characteristics will only be used to assist the production of Equality Impact Assessments or similar monitoring on records of racial or social equality.
- Scenario modelling – identifying the impacts of changes in activity and clinical models on affected staff groups.

3 – ***Adequate, relevant and not excessive***:

- Throughout the development of WRaPT, the data has been assessed to ensure it is adequate, relevant and not excessive. Each mandatory field required for WRaPT is vital in order to produce any meaningful workforce analysis or modelling, additional optional fields are relevant for further analysis such as Equality Impact Assessments.

4 - ***Accurate and up to date***:

- Data is refreshed once per year, and is requested to be refreshed before new modelling is undertaken. Data is, in most cases, entered from a download from ESR or other staff record system. We encourage all WRaPT users to validate any data for modelling or analysis with a secondary source, such as finance data, and/or by communicating with the teams involved.

5 – ***Not kept longer than is necessary***:

- Data in the repository is held for a maximum of one year unless refreshed.

6 – ***Processed in line with the subject's data rights***:

- As well as following LCFT data access processes, we remove any data upon notification of the subject's objection to it being used within WRaPT. We ask each system to note on their website, following normal Data Protection processes within their organisations, to make staff aware that data is being used across systems for workforce planning purposes and to inform them of the appropriate procedure for Subject Access Requests and data updates or objection to processing.

7 – ***Secure***:

- Data is transmitted password protected, with a separate communication method required for the password, usually SMS message. The WRaPT system is subject to penetration testing. Access within an organisation is granted by a suitable party who is nominated as a "Super User", this individual is able to assign an appropriate access to individuals within their organisation. Additionally, the system has a series of role based access controls restricting users to appropriate sections of the workforce and data fields.

8 – ***Not transferred to other countries without adequate protection***:

- WRaPT data is not held outside the EEA except where there is a current safe harbour agreement.

Data updates

The data held within the system must be updated at least annually, or it is removed. Prior to any system project, systems receive a communication from the WRaPT team asking them to update their data.

DPA roles

The following specific roles are in place:

- Lancashire Care SIRO – Finance Director
- Lancashire Care Caldecott Guardian – Medical Director
- GE Healthcare Finnamore SIRO – Liaises with Lancashire Care DP staff, and works to ensure that GEHCF specific issues are addressed – Colin Lewry
- WRaPT "SIRO" – Liaises with Lancashire Care DP staff to help ensure WRaPT risks are considered and controlled within Lancashire Care – Colin Lewry
- WRaPT "guardian" – Supports WRaPT SIRO with ensuring that data protection is a core part of daily processes within the WRaPT team – Robert Mulligan

Data protection training

All staff and team members involved with WRaPT from LCFT and GE complete the HSCIC (or equivalent) IG Training modules on an annual basis.

Data retention

We hold WRaPT data for a maximum of one year, at which point it must either be refreshed or deleted in line with the Lancashire Care NHS Foundation Trust policy for deletion of data.

Access to the system

As well as the individual parties, only the following organisations have access to the system:

- HEE – As per the Health and Social Care Act 2012

- Lancashire Care NHS Foundation Trust staff associated with the project and IT systems.
- GE Healthcare Finnamore
- Mando Group (to 31st March 2018)
- 01 Group (as software developers)
- Rackspace (as WRaPT website hosting service)

Data locations

Data is held in the following locations:

- Laptops - These must only be encrypted laptops. Staff must only hold data related to the specific projects that they are engaged in, for the duration they are in use, as noted by the WRaPT Manager.
- LCFT data storage - One single version of the original data, and one version of amended data (if required) is held in the specific project file for each system implementation.
- WRaPT File Share System – Secure cloud storage hosted on a Health Education England server within the UK, this is used primarily for file access for remote workers.
- WRaPT servers – Backup, live.

Subject Access Request policy

In accordance with the LCFT Access to Health Records policy subject access rights include:-

- To be informed whether personal data is being "processed". Processing includes the collection, use, storage, disclosure and subsequent destruction of information relating to living individuals
- To be provided with a description of the data held, the purposes for which it is processed and a description of those to whom the data is or may be disclosed
- To be provided with a copy of the information constituting the data within 20 working days of the Trust receiving the application
- To be provided with information to identify the source of the data

Upon receipt of any Subject Access Requests these are to be forwarded to the WRaPT Guardian who will produce and send a response.

Information asset management

Information Assets related to the WRaPT Service are recorded on the LCFT Information Asset Register. The register is reviewed regularly to ensure risks to the information are mitigated appropriately.

Process for handling dissent

All team members should be aware that any dissent identified by an individual or organisation should be immediately raised with the WRaPT Service Manager or lead. Information is to be deleted or amended as requested.

Privacy Impact Assessment

Because WRaPT collects, stores and reports on data that is potentially personally identifiable, we have undertaken a Privacy Impact Assessment (PIA) to assure not only ourselves as a service that we understand, minimise and manage any risks around individuals' or groups of individuals' data but also so we can re-assure the organisations that we work with of the same.

A copy of the PIA can be found at Appendix 2.

System Penetration Testing

In March 2016 the WRaPT System was subjected to an Independent System Penetration Test. This test was undertaken by NCC Group PLC who specialise in security testing audit and compliance. The scope of the test covered 1) External Infrastructure Assessment of the host that supports the web application and 2) Web Application Assessment of the WRaPT application.

Prior to full migration to the new version of the WRaPT System an Independent Penetration Test will be carried out to the above specification.

Data Sharing Agreements

When sharing data between organisations it is crucial to ensure that information is transmitted, stored and processed appropriately and as such we ensure data sharing agreements are signed at all necessary points. With many of our partner organisations we look to make use of the Information Sharing Gateway (ISG) which enables an efficient and streamlined way to progress data sharing agreement and sign-off. Alternatively we have Tier 1 and Tier 2 Data Sharing Agreements that we use with cross-economy transformation programmes whereby all partners sign up to the data sharing principles outlined within.

The Tier 1 sets out the agreement between all the parties in a cross-economy programme to share data between themselves for the purpose of using WRaPT. Sign-up to the Tier 2 agreement enables WRaPT to receive, process and produce reports on data in WRaPT. Without such agreements in place, the justification for receiving workforce information into

WRaPT is diminished along with the opportunities to fully implement WRaPT to the benefit of the partner organisations.

A single-organisation agreement is also available which allows sign-up from one e.g. health or social care organisation to work with WRaPT on a smaller scale or within organisation project.

Copies of the sample Tier 1, Tier 2 and Single-Organisation Data Sharing Agreements can be found at Appendix 3, 4, & 5 respectively.

WRaPT IG Key Contacts

Colin Lewry – SIRO, GE Healthcare Finnamore

Colin.lewry@ge.com

Robert Mulligan – SIRO (WRaPT) & IG Lead, GE Healthcare Finnamore

Robert.Mulligan@ge.com

Fiona Lord – WRaPT Service Manager, Lancashire Care NHS Foundation Trust

Fiona.lord@lancashirecare.nhs.uk

APPENDICES

Number	Detail	
1.	LCFT Data Sharing Policy	
2.	Privacy Impact Assessment	
3.	Tier 1 – Sample Data Sharing Agreement*	
4.	Tier 2 – Sample Data Sharing Agreement*	
5.	Single-Organisation Data Sharing Agreement*	

*These sample documents are provided as reference material only and as such should not be used without prior confirmation from organisations' internal Information Governance function.