Rescon Ltd
Data Collection, Management and Processing Policy

Revision History

Version	Revision Date	Summary of Changes	Author
1.0	15/08/2018	Document creation	Tom Dawson

Table of Contents

1. Introduction

Rescon is committed to providing high standards of information governance, and ensuring appropriate policies, procedures and structures provide a robust framework for information collection, management and processing.

2. Scope

This policy outlines the information collected, managed and processed where personal data is collected directly and indirectly including Rescon's health and care management platform Lincus.

3. Information Governance Statement

In accordance with the General Data Protection Regulation (GDPR) information provided (referenced below):

- Will be protected by national and international laws
- Will be used for the best interests of data subjects
- May be shared with health and social care systems and services
- May be used for service improvement and research in the public interest
- Will be provided to the data subject on request
- Will never be shared with or sold to third parties for direct commercial gain
- Is controlled and/or processed by Rescon Ltd, a UK company registered with the Information Commissioner's Office (www.ico.org.uk) depending on how the service has been commissioned with the relationship outlined in a Service Level Agreement if commissioned by an organisation

4. Data Collection

Data collected is relevant to help users of Rescon service live the healthiest life possible. The primary purpose of the service is to provide a secure data repository for personal data that is led by the data subject. In keeping with this purpose the majority of data can be entered at the discretion of the user and the source of data collected is logged.

Users must provide, at a minimum, the following information during registration:

- A valid personal email address
- Password
- Gender
- Confirmation that they are at least 16 years of age

To provide the best service possible including for verification purposes, the following data may be collected:

- Web browser type and version
- Operating system
- Cookie information
- An identification photo*
- Confirmatory personal identification information such as date of birth, phone number or an address*
- A video statement*
- A digital verification certificate from a previous validated user such as a health or social care worker*

* Requirements at the time of publication for NHS Citizen ID Scheme

All other data can be entered at the discretion of the user which may include:

- Name
- Date of birth
- Contact information
- Physical or mental health information
- Self-reported health and wellbeing

www.rescontechnologies.com
info@rescontechnologies.com
penn croft farm – the carthouse, farnham, surrey GU10 5PX

- Interests
- Forename
- Surname
- Address
- Post code
- Date of birth (age)
- National Insurance Number
- Educational information
- Employment information
- Data subject location
- Telephone number
- IP address
- Other unique identifiers
- Racial or ethnic origin
- Religious or ethnic origin

Observed, derived or inferred data can be collected with the source of this information logged including:

- Observed health and wellbeing
- Device or application information (e.g. activity tracker)
- Health, wellbeing and social information (e.g. diagnoses, medical history, social care history)

5. Data Management

In accordance with the GDPR data submitted will be:

- Protected by national and international laws
- Used for the best interests of the data subject
- Retained by Rescon indefinitely for reasons of best interest of the data subject, public interest, scientific research and legal defence claims
- Stored securely in the EU
- Controlled with suitable physical, electronic and management procedures
- Pseudonymised/anonymised where possible to protect personal data

In accordance with the GDPR data submitted may be:

- Shared with health and social care systems and services (but only for the best interest of that data subject or if there is another legal basis such as safeguarding)
- Used for research and public interest

All information systems and data are hosted on secure cloud servers. Only named authorised personnel have access to these environments through a combination of username, password and private keys.

www.rescontechnologies.com
info@rescontechnologies.com
penn croft farm – the carthouse, farnham, surrey GU10 5PX

De-identification

Pseudonymisation/anonymisation removing personal data identifiers (PID) must be used where possible protect personal data. Information which has had personal identifiers removed or replaced in order to pseudonymize the data is still personal data for the purposes of GDPR. Information which is truly anonymous is not covered by the GDPR.

Consideration must be given to combining data sets that may result in an individual being able to be identified. For any aggregation there must be at least six in each group to protect the identity of any individual data subject. If there are fewer than these then the field must be pseudonymised (as below).

Pseudonymisation

When pseudonymisation techniques are consistently applied, the same pseudonym must be provided for individual data subjects across different data sets and over time. This allows the linking of data sets and other information which is not available if the PID is removed completely.

To effectively pseudonymise data the following actions must be taken:

- Each identifying field of PID must have a unique pseudonym;
- Pseudonyms to be used in place of NHS numbers and other unique identifiers and other fields must be of the same length and formatted on output to ensure readability. For example, in order to replace NHS Numbers in existing report formats, then the output pseudonym should generally be of the same field length, but not of the same characters; i.e. 5L7 TWX 619Z. Letters should be used within the pseudonym for an NHS number to avoid confusion with original NHS numbers;
- Consideration needs to be given to the impact on existing systems both in terms of the maintenance of internal values and the formatting of reports;
- Where used pseudonyms for external use must be generated to give different pseudonym values in order that internal pseudonyms are not compromised;
- The secondary use output must, where pseudonyms used, only display the pseudonymised data items that are required. This is in accordance with the Caldicott Guidelines;
- Pseudonymised data must have the same security principles applied as PID as pseudonymised data is still considered personal data for the purposes of GDPR.

Data Retention, Archive and Deletion

Management of information records including retention, archive and deletion are outlined in the Records Management Policy.

6. Data Processing

In accordance with the GDPR data is processed by Rescon Ltd on the following lawful bases:

www.rescontechnologies.com
info@rescontechnologies.com
penn croft farm – the carthouse, farnham, surrey GU10 5PX

Primary

- Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract (Article 6 - 1b)

Secondary

- Processing is necessary for compliance with a legal obligation to which the controller is subject (Article 6 – 1c)
  Processing is necessary in order to protect the vital interests of the data subject or of another natural person (Article 6 – 1d)
  Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller (Article 6 – 1e)

In accordance with the GDPR special category data is processed by Rescon Ltd on the following lawful bases:

Primary - Active

- Processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3 (Article 9 – 2h)

Secondary

- Processing is necessary to protect the vital interests of the data subject or another person (Article 9 – 2c)
- Processing relates to personal data which are manifestly made public by the data subject (Article 9 – 2e)
- Processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity (Article 9 – 2f)
- Processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject (Article 9 – 2g)
- Processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy (Article 9 – 2i)

www.rescontechnologies.com
info@rescontechnologies.com
penn croft farm – the carthouse, farnham, surrey GU10 5PX

- Processing is necessary for archivingarching purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject (Article 9 – 2j)

Processing Personal Data

Personal data means any information relating to an identified or identifiable natural person (data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Processing Special Category Data

Special category data refers to more sensitive personal data which requires maximal protection including:

- Race
- Ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetic data
- Biometric data (where it is used for identification purposes)
- Health data
- Sex life
- Sexual orientation
- Criminal convictions and offences

To ensure special category data is maximally protected, wherever possible, this data is flagged. The exception to this is where special category data may be entered as free text and cannot necessarily be identified.

There must be a valid lawful basis in order to process personal data. Individuals must be provided with information on the basis for processing special category data. If no lawful basis applies to the processing, processing will be unlawful and in breach of the GDPR.

Processing Pseudonymised Data

Pseudonymisation is the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to

www.rescontechnologies.com
info@rescontechnologies.com
penn croft farm – the carthouse, farnham, surrey GU10 5PX

an identified or identifiable natural person. Pseudonymising personal data can reduce the risks to data subjects.

Pseudonymisation may involve replacing names or other identifiers which are easily attributed to individuals, for example with a reference number. As this reference number can be tied back to the individual there must be appropriate measures in place to ensure that this information is held separately and securely.

Information which has had personal identifiers removed or replaced in order to pseudonymise the data is still personal data for the purposes of GDPR. Therefore, there must be a valid lawful basis in order to process the data. If no lawful basis applies to the processing, processing will be unlawful and in breach of the GDPR.

Processing Anonymised Data

Anonymised data does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. Caution must be exercised when anonymising personal data. Information which is truly anonymous is not covered by the GDPR. In order to be truly anonymised, all personal data must be stripped to mean that the individual can no longer be identified (and cannot be re-identified in any way). When data is anonymised, the data is still being processed at that point and therefore there must be a valid lawful basis for processing the data. Anonymisation wherever possible is encouraged to limit risk to data subjects.

7. Contact Details

Data Controller

Name	Rescon Ltd
Email	info@rescon.eu
Phone	07540 164555
Address	The Kilns, Penn Croft Farm, Crondall, Surrey GU10 5PX

Data Protection Officer

Name	Data Protection Officer
Email	dpo@lincus.eu

8. Review & Monitoring

This policy must be reviewed and approved at least annually. Compliance with the Data Collection, Management and Processing Policy will be monitored with at least annual audits and ongoing monitoring by the Information Governance Committee.

9. Policy Approval

This policy has been reviewed and approved the Information Governance Lead.

Name: Tom Dawson

Position: Managing Director and Information Governance Lead

Date: 06/09/2018

Signature: 

www.rescontechnologies.com
info@rescontechnologies.com
penn croft farm – the carthouse, farnham, surrey GU10 5PX