Rescon Ltd
Data Protection By Design Policy

Revision History

Version	Revision Date	Summary of Changes	Author
1.0	16/08/2018	Document creation	Tom Dawson

Table of Contents

1. Summary

It is paramount to ensure that information is effectively managed, and that appropriate policies, procedures and management accountability and structures provide a robust framework for information management. Systems must be designed to ensure protection and security of data from the point of conception throughout the design and implementation phases. Data protection is an essential function of Rescon systems.

2. Scope

This document applies to all Rescon system and service developments from conception through to the design and implementation.

3. Principles

Privacy first

A privacy first approach must be adopted to ensure default settings of systems/services address privacy first and foremost. Data protection must be considered as a core function within systems/services.

Minimal data

Rescon systems must process and display only the minimum necessary personal data. No more data than is needed for the identified purpose should be held or displayed.

De-identification

Pseudonymisation/anonymisation removing personal data identifiers (PID) must be used where possible protect personal data. 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.

Transparency

Where possible, individuals must be able to access the information that is held about them and what is being done with their data. This can be accessed through relevant transparency information which is available to the public. Users must also be made aware of this information through the terms and conditions of systems/services.

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

When it is in the best interest of the data subject to not have access to the information, such as for safeguarding, then this must be clearly documented both internally and for the end user.

For example:

Clinical view: “This data is protected until clinically reviewed as the findings may have a negative impact on the health and wellbeing of the patient. Please review as soon as possible and discuss with the patient.”

Data subject view: “Your blood test result is not available yet as it is undergoing medical review. Please contact your medical team for further information.”

Risk assessment

Risks are assessed during the early stages of system/service design to ensure risk is of an acceptable/tolerable level with relevant mitigations in place. Data Protection Impact Assessments (DPIA), Privacy Impact Assessments (PIA) and Change Control documentation must be completed to minimise risk prior to implementation and commencement of processing.

Security

All systems/services must protect personal data automatically, without requiring the individual to take any specific action.

Plain language

Plain language must be used for any public documents to enable people to easily understand how their data is protected and used.

4. Review & Monitoring

This policy must be reviewed at least annually. Compliance with the Data Security and Protection By Design policy will be monitored with at least annual audits and ongoing monitoring by the Information Governance Committee.

5. Policy Approval

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

Name: Tom Dawson

Position: Managing Director and Information Governance Lead

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

Date: 06/09/2018

Signature: 

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