Rescon Ltd
Data Security and Protection Policy

Revision History

Version	Revision Date	Summary of Changes	Author
1.0	20/10/2018	Data Security and Protection Policy created merging Information Governance and Confidentiality Policies for NHS Digital Data Security & Protection Toolkit	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 governance framework for information management. This policy is required to safeguard and protect personal identifiable information within the organisation and when it is in transit.

All staff must be aware of their responsibilities for safeguarding personal information and preserving information security. All Rescon employees are bound by a legal duty of confidence to protect personal information they may come into contact with during the course of their work. This is not just a requirement of their contractual responsibilities but also a requirement within the General Data Protection Regulation (GDPR) and Data Protection Act 2018.

2. Scope

The scope of this document applies to all Rescon staff and subcontractors, including those on permanent, temporary, flexible and fixed term contracts.

3. Principles

Rescon aims to implement information governance effectively and will ensure the following:

- Personal information must be protected against unauthorised access or improper disclosure when it is received, stored, transmitted or disposed of
- Data security and protection must be assured
- Integrity of information will be maintained
- Information will be supported by the highest quality data
- Regulatory and legislative requirements will be met
- Information governance training will be available to all staff as necessary
- All breaches of confidentiality and information security (actual or suspected) will be reported and investigated
- Access to person identifiable or confidential information must be on a need-to-know basis
- Disclosure of person identifiable or confidential information must be limited to that purpose for which it is required
- Recipients of disclosed information must respect that it is given to them in confidence
- If the decision is taken to disclose information that decision must be justified and documented

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

- Any concerns about disclose must be discussed with the Information Governance Committee
- Person identifiable information must be anonymised or pseudonymised wherever possible, removing as many identifiers as possible whilst not unduly compromising the utility of the data

In line with the GDPR, there are 7 key principles which must be complied with:

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality (security)
- Accountability

Lawfulness, fairness and transparency

Rescon will ensure:

- There are appropriate lawful bases for data processing
- There are conditions for processing special category data
- Personal data is not used unlawfully
- How processing may affect the individuals and justification for any adverse impact has been considered
- Data is handled in a way that would be reasonably expected
- People are not deceived or misled when their personal data is collected
- Openness, honesty and clarity with how personal data is used

Purpose limitation

Rescon will ensure:

- Purposes for processing are clearly identified, documented and made available to individuals
- Purposes for processing are regularly reviewed and when necessary documentation is updated
- When planning to use personal data for a new purpose, checks are made to ensure it is compatible with the original purpose for processing

Data minimisation

Rescon will ensure that personal data that is processed is:

- Adequate to fulfil the stated purpose
- Relevant to that purpose
- Limited to what is necessary for that purpose

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

Accuracy

Rescon will ensure:

- Accuracy of personal data created
- Appropriate processes are in place to check the accuracy of data collected including recording the source of the data
- Processes are in place to identify when the data needs to be updated to fulfil the purpose of processing
- If records of mistake are kept, they are clearly identified as a mistake
- Records clearly identify any matters of opinion and where appropriate whose opinion it is an any changes to the underlying facts
- Compliance with the individual's right to rectification and carefully consider any challenges to the accuracy of the personal data
- A note is kept of any challenges to the accuracy of personal data

Storage limitation

Rescon will ensure:

- Personal data is not kept for longer than it is needed including justification for holding personal data
- A policy is in place detailing data retention periods
- Information is regularly reviewed, with data archived or anonymised when no longer needed
- Appropriate processes are in place to comply with individuals' requests for erasure under the right to be forgotten
- Personal data that is kept for public interest archiving, scientific or historical research, or statistical purposes is clearly identified

Integrity and confidentiality (security)

Rescon will ensure:

- There are appropriate security measures in place to protect the personal data that is held

Accountability

Rescon will ensure:

- Responsibility for what is done with personal data and how the principles are complied with
- Appropriate measures and records are in place to be able to demonstrate compliance with the principles

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

4. Organisational Roles & Responsibilities

It is the role of Rescon to define the company's policy in respect of information governance, taking into account legal requirements. Rescon is also responsible for ensuring that sufficient resources are provided to support the requirements of this policy.

Rescon's Information Governance Committee is responsible for overseeing day to day Information Governance issues; developing and maintaining policies, standards, procedures and guidance, coordinating Information Governance and raising awareness of Information Governance. Contact details for the Information Governance Committee are detailed in section 11.

Managers within Rescon are responsible for ensuring that the policy and its supporting standards and guidelines are built into local processes and that there is ongoing compliance.

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

Named individuals will take responsibility for co-ordinating, publicising and monitoring standards of information handling within the organisation and for developing and implementing an Information Governance improvement plan.

All staff and contractors will be used as a resource for ongoing and continuous quality improvement for all company practices. They will be encouraged to contribute to and make suggestions around methods and refinements that could be implemented to improve information governance processes.

3.1 Information Governance Lead

The Information Governance Lead is accountable for ensuring effective management, accountability, compliance and assurance for all aspects of information governance.

Key responsibilities include:

- Developing and maintaining the currency of comprehensive and appropriate documentation that demonstrates commitment to and ownership of information governance responsibilities, e.g. an overarching high-level strategy document supported by corporate and/or directorate policies and procedures
- Ensuring that there is top level awareness and support for information governance resourcing and implementation of improvements
- Providing direction in formulating, establishing and promoting information governance policies
- Establishing working groups, if necessary, to co-ordinate the activities of staff given information responsibilities and progress initiatives

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

- Ensuring annual assessments using the Data Security and Protection Toolkit and audits of policies and arrangements are carried out, documented and reported in line with the requirements of the NHS Standard Contract
- Ensuring that the annual assessment and improvement plans are prepared for approval by the senior level of management, e.g. the board or senior management team in a timely manner. For example, for NHS Trusts, sign off may be scheduled in advance of the end of financial year submission on the 31 March each year
- Ensuring that the approach to information handling is communicated to all staff and made available to the public
- Ensuring that information governance staff understand the need to support the safe sharing of personal data for direct care as well as the need to protect individuals' confidentiality
- Ensuring that appropriate training is made available to all staff and completed as necessary to support their duties. For NHS organisations, this will need to be in line with the mandate for all staff to be trained annually and should take into account the findings of the National Data Guardian review 'Recommendations to on the Review of data security, consent and opt-outs and ensure people can make informed choices about how their data is used. 'Information: to share or not to share?

3.2 Senior Information Risk Owner (SIRO)

The Senior Information Risk Owner (SIRO) is responsible for ensuring information security risks are followed up and incidents managed.

Key responsibilities include:

- Oversee the development of an Information Risk Policy and a strategy for implementing the policy within the existing Information Governance Framework
- Take ownership of the risk assessment process for information and cyber security risk, including review of an annual information risk assessment to support and inform the Statement of Internal Control
- Review and agree action in respect of identified information risks
- Ensure that the organisation's approach to information risk is effective, in terms of resource, commitment and execution and that this is communicated to all staff
- Provide a focal point for the resolution and / or discussion of information risk issues
- Ensure the board is adequately briefed on information risk issue
- Ensure that all care systems information assets have an assigned Information Asset Owner

3.3 Caldicott Guardian

The Caldicott Guardian is responsible for protecting the confidentiality of people's health and care information and making sure it is used properly.

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

3.4 Data Protection Officer (DPO)

The DPO must inform and advise about compliance with GDPR and other data protection laws, monitor compliance with GDPR and data protection laws including staff training and internal audits, advise on and monitor data protection impact assessments, cooperate with the ICO and be the first point of contact for the ICO and public in terms of data processing.

3.5 Other Staff

All staff working on behalf of the organisation are responsible for ensuring that they are aware of their responsibilities relating to the Data Security and Protection Policy. All employees working in Rescon are bound by a legal duty of confidence to protect personal information they may come into contact with during their course of work.

Staff must complete an information governance induction, in addition to training and awareness meetings. Any data security of protection incidents must be reported immediately. Any breach of confidentiality could result in dismissal or termination of employment.

Staff must advise a member of the Information Governance Committee if they identify areas where improvements to information governance processes or documentation can be made.

4. Key Policies

Rescon will provide a number of policies (or equivalent) to set out scope and intent in terms of embedding Data Security and Protection processes throughout the organisation:

The Information Governance Committee will ensure:

- Comprehensive and appropriate documentation is developed and maintained to demonstrate commitment to and ownership of information governance responsibilities
- Senior management awareness and support for information governance resourcing and implementation of improvements
- Direction provided in formulating, establishing and promoting information governance policies
- Working groups established if necessary to co-ordinate the activities of staff given information governance responsibilities
- Assessment and improvement plans are prepared for approval in a timely manner and in line with national reporting requirements
- The approach to information handling is communicated to all staff and made available to the public
- Appropriate training is made available to staff and completed as necessary to support their duties
- Policies are in place for data collection, management, processing, retention, archive and deletion

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

- Information handling is monitored to ensure compliance with information governance guidance
- A focal point is provided for resolution and/or discussion of information governance issues

Key policies include:

- Acceptable Use Policy
- Data Collection, Management and Processing Policy
- Data Protection By Design Policy
- Data Quality Policy
- Records Management Policy
- System Security Policy
- User Rights Policy

5. Types of Data

It is important to be able to identify the different types of information so they can be appropriately protected when they are used and shared.

Personal Data

According to the GDPR, 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.

Special Category Data

According to the GDPR, special category data refers to more sensitive personal data which requires a higher level of 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

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

Pseudonymised Data

According to the GDPR, pseudonymised data is data that can no longer be attributed to a specific data subject without the use of additional information such as a reference number which must be kept separately and is subject to technical and organisational measures. Pseudonymised data is still considered personal data for the purposes of GDPR.

Anonymised Data

According to the GDPR, anonymised data is information which 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. Anonymised data is not subject to the GDPR and is encouraged wherever possible.

6. Disclosing Personal Information

To ensure that information is only shared with the appropriate people in appropriate circumstances, care must be taken to check they have a legal basis for access to the information before releasing it.

Information can be disclosed when:

- For the care of and/or treatment of an individual by a suitably qualified individual or organisation where permission explicit, implicit or otherwise has been given
- Effectively anonymised
- The information is required by law or under court order. In this situation staff must discuss with the Information Governance Committee before disclosing
- In identifiable form, when it is required for a specific purpose, with the individual's written consent
- In Child Protection proceedings if it is considered that the information required is in the public or child's interest. In this situation staff must discuss with the Information Governance Committee before disclosing
- Where disclosure can be justified for another purpose, usually for the protection of the public and is likely to be in relation to the prevention and detection of serious crime. In this situation staff must discuss with the Information Governance Committee before disclosing

If staff have any concerns about disclosing information they must discuss this with the Information Governance Committee.

Care must be taken in transferring information to ensure that the method used is as secure as it can be. In most instances a Data Sharing, Data Re-Use or Data Transfer Agreement will have been completed before any information is transferred. The Agreement will set out any conditions for use and identify the mode of transfer. For further information on data sharing contact the Information Governance Committee.

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

Staff must ensure that appropriate standards and safeguards are in place in respect of telephone enquiries, emails, faxes and surface mail.

Transferring personal information by email may only be undertaken by using encryption, to ensure that mandatory government standards on encryption are met. Sending information via email to users is permissible, provided the risks of using unencrypted email have been explained to them, they have given their consent and the information is not person identifiable.

7. Secure Working Practices

Staff must ensure safe and secure working practices, particularly when working from home or whilst traveling. Personal information must be safeguarded at all times and staff have personal responsibility for ensuring personal information is kept secure. Do's and Don'ts relating to secure working practices are outlined in Appendix A.

8. Training Guidance

Staff must be given clear guidelines on expected working practices and the consequences of failing to follow policies and procedures. Staff must complete Data Security and Protection training during their induction. Staff must also complete self-directed study to ensure compliance with policies and processes. Staff are required to report back on an annual basis with a synopsis of formal and self-directed data security and protection training over the year including key points learned and useful resources. Training needs will be analysed with appropriate training provided in response.

9. Incident Management

Clear guidance on incident management procedures are documented and staff are made aware of their existence, where to find them and how to implement them. An incident reporting policy has been created and made available to all staff. Staff will be made aware of the importance of reporting actual incidents or near misses during data security and protection training.

10. Sanctions and Abuse of Privilege

All staff have a legal duty of confidence to keep person identifiable or confidential information private and not to divulge information accidentally. Staff may be held personally liable for a breach of confidence and must **not**:

- Talk about person identifiable or confidential information in public places or where they can be overheard
- Leave any person identifiable or confidential information unattended, including telephone messages, computer printouts, faces and other documents

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

- Leave a computer terminal logged on to a system where person identifiable or confidential information can be accessed, unattended
- Access of attempt to gain access to unauthorised information

Breach of this policy could lead to disciplinary action. Depending on the circumstances, this could range from remedial training to dismissal.

It is strictly forbidden for employees to knowingly browse, search for or look at any information relating to their own family, friends or other persons without a legitimate purpose. Action of this kind will be viewed as a breach and deemed a disciplinary offence.

When dealing with personal information of any nature, staff must be aware of their personal responsibility, contractual obligations and undertake to abide by the policies and procedures of Rescon.

11. Distribution

This policy will be made available to all Rescon staff.

12. Contacts

Information Governance Lead	Tom Dawson	tom.dawson@rescontechnologies.com
Senior Information Risk Owner (SIRO)	Chris Milner	chris.milner@rescontechnologies.com
Caldicott Guardian	Adie Blanchard	adie.blanchard@rescontechnologies.com
Head of IT	Laura Gilbert	laura.gilbert@rescontechnologies.com

13. Review & Monitoring

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

14. Policy Approval

Rescon acknowledges that information is a valuable asset, therefore it is wholly in its interest to ensure that the information it holds, in whatever form, is appropriately governed, protecting the interests of all its stakeholders.

This policy and its supporting standards and work instruction, are fully endorsed through the production of these documents and their minuted approval.

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

All staff, contractors and other relevant parties will ensure that these are observed in order to contribute to the achievement of Rescon's objectives.

Information Governance Lead: /tom dawson/ Date: 20/10/2018

Appendix A: Data Security and Protection Do's and Don'ts

Do:

- Safeguard all person identifiable information that you come into contact with
- Keep all personal information in recognised filing and storage places that are locked when access is not controlled or supervised
- Password protect computers with access to personal information, particularly if leaving the computer for any length of time
- Ensure that you cannot be overheard when discussing confidential matters
- Challenge and verify where necessary the identity of any person who is making a request for personal information and ensure they have a need to know
- Justify any decision to share information and check there is a legal basis for doing so before sharing any information
- Ensure information is only shared with appropriate people in appropriate circumstances using appropriate measures (i.e. encrypted email transfer)
- Share only the minimum amount of information necessary
- Transfer personal information securely and only when necessary
- Seek advice from the Information Governance Committee prior to sharing personal information
- Report actual or suspected breaches of data security and protection
- Participate in induction, training and awareness raising sessions on information governance
- Anonymise information where possible, particularly before sharing

Don't:

- Share passwords or leave them lying around for others to see
- Share personal information with anyone if there is not a lawful basis for doing so
- Share information without the consent of the person to which the information relates, unless there are statutory grounds to do so
- Use personal information unless absolutely necessary (anonymise where possible)
- Collect, hold or process more information that you need, and do not keep it for longer than necessary
- Remove documentation containing personal information from secure premises unless necessary to do so
- Forward or send any emails containing personal information to home email accounts
- Store personal information on a privately owned computer or device

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

- Leave personal information unattended including phone messages, computer printouts, documents
- Leave devices logged in to a system where personal information can be accessed

Appendix B: Guiding Principles

This policy is guided by the following legislations:

- **The Data Protection Act 2018** which regulates the use of personal data and sets out eight principles to ensure that personal data is:
    - Processed fairly and lawfully
    - Processed for specified and lawful purposes
    - Adequate, relevant and not excessive
    - Accurate and where necessary kept up to date
    - Not kept longer than necessary, for the purpose it is used
    - Processed in accordance with the rights of the data subject under the Act
    - Appropriate technical and organisational measures are to be taken to guard against unauthorised or unlawful processing, accidental loss or destruction of, or damage to, personal data
    - Not transferred to countries outside the European Economic Area (EEA) without an adequate level of protection in place
- **The Caldicott Report (1997)** which recommended that a series of principles be applied when considering whether confidential identifiable information should be shared:
    - Justify the purpose for using personal identifiable information
    - Don't use identifiable information unless absolutely necessary
    - Use the minimum necessary personal identifiable information
    - Access to personal identifiable information should be on a strict need to know basis
    - Everyone must be aware of their responsibilities
    - Understand and comply with the law
- **Article 8 of the Human Rights Act (1998)** which refers to an individual's 'right to respect for their private and family life, for their home and for their correspondence'
- The **Computer Misuse Act (1990)** which makes it illegal to access data or computer programs without authorisation and establishes three offences
    - Unauthorised access to data or programs held on a computer to view information for a person who's care you are not directly involved in or to obtain or view information about friends and relatives
    - Unauthorised access with the intent to commit or facilitate further offences e.g. fraud or blackmail
    - Unauthorised acts the intent to impair, or with recklessness so as to impair, the operation of a computer e.g. to modify data or programs held on computer without authorisation
- **Common Law Duty of Confidentiality**

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

  - There must be a lawful basis for the use or disclosure or personal information that is held in confidence
  - Those not directly involved in an individual's care cannot assume they can access confidential information about the individual in a form that identifies them
- **Administrative Law**
- **The General Data Protection Regulation (2018)** which sets out the following seven key principles:
  - Lawfulness, fairness and transparency
  - Purpose limitation
  - Data minimisation
  - Accuracy
  - Storage limitation
  - Integrity and confidentiality (security)
  - Accountability

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