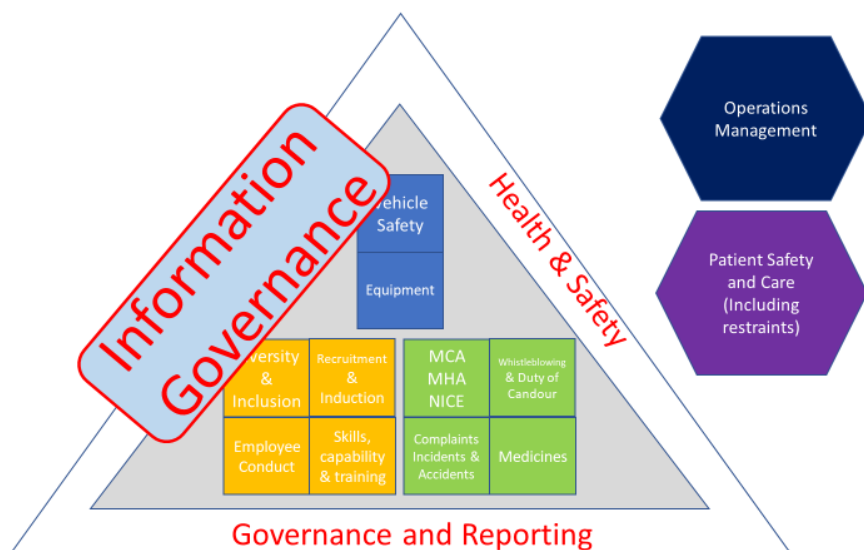


Secure Care UK Policy Framework

Policy Title: Information Governance



SECURE CARE UK
SECURE PATIENT TRANSPORT SPECIALISTS

Approved: _____
Finance and IT Manager

Last Reviewed Date:

Approved: _____
Managing Director

Last Reviewed Date:

1.0 Purpose

1. This policy has been prepared and published mindful of our obligations to our colleagues, patients and NHS Clients. We are mindful that information governance is covered by UK and EU legislation and believe that to the best of our ability the approaches outlined within this policy enable our full compliance with our obligations. The purpose of the policy is to establish general standards for Information Governance including all aspects of data protection and information systems management and to distribute responsibility for their achievement to all managers, supervisors, and other employees through the normal line management processes.

2.0 Scope

2.1 The scope of this policy will cover all of the business activities undertaken by Secure Care UK including the management supplier and sub contracting relationships. This policy applies to all employees within the organisation and also identifies where particular responsibilities are assigned to members of the management structure.

2.2 This policy, together with the associated standards, applies to the management of all documents and records, in all technical or physical formats or media, created or received by the ICO in the conduct of its business activities. It applies to all staff, contractors, consultants and third parties who are given access to our documents and records and information processing facilities.

- *Data Protection Act 1998*
- *Freedom of Information Act 2000*
- *Health & Social Care (Safety & Quality) Act 2015*
- *Computer Misuse Act 1990*

2.3 The nature of the activity undertaken by Secure Care UK necessitates the use of CCTV for the protection of our colleagues and patients. This policy will include within its scope the management of the images and recordings from any CCTV systems.

2.4 The table below provides a listing of the tangible and intangible assets impacted by this policy.

Personal Information Content	Software
- Databases and data files - Back-up and archive data - Audit data - Paper records (patient case notes and staff records) - Paper reports	- Applications and System Software - Data encryption utilities - Development and Maintenance tools
Other Information Content	Hardware
- Databases and data files - Back-up and archive data - Audit data - Paper records and reports	Computing hardware including PCs, Laptops, PDA, communications devices eg. blackberry and removable media
System/Process Documentation	Miscellaneous
- System information and documentation - Operations and support procedures - Manuals and training materials - Contracts and agreements - Business continuity plans	- Environmental services eg. power and air-conditioning - People skills and experience - Shared service including Networks and Printers - Computer rooms and equipment - Records libraries

3.0 Responsibilities

- 3.1 It is the responsibility of the Managing Director to review this document and to recommend its approval to the board. As Secure Care UK is a relatively small organisation the Managing Director will undertake the duties of Caldicot Guardian supported by our main board Clinical Advisor.
- 3.2 Our Finance and IT Manager will be accountable for the implementation of this policy and will act as the Serious Information Risk Owner (SIRO) and the Data Protection Officer
- 3.3 The Quality Manager will monitor the delivery of all audits described within this policy and ensure that the Governance Committee and board review all audits and instruct the management team to take actions as a result of these audits.
- 3.4 It is the responsibility of all employee with any management responsibilities to ensure that the requirements of this policy are communicated, trained and where necessary, enforced.
- 3.5 It is the responsibility of all employees at Secure Care to follow this policy and these obligations will be made clear in all contracts of employment.

4.0 Definitions

- 4.1 SOP's – Standard Operating Procedures
- 4.2 SIRO – Serious Incident Risk Manager

5.0 Related Documents

- 5.1 Employee Handbook
- 5.2 SOPs
- 5.3 Register of systems

- 5.4 Business Continuity Plan
- 5.5 Data Protection Impact Assessment Tool (Appendix 1)
- 5.6 Transparency Statement (Appendix 2)
- 5.7 Staff Information Security Guidance

6.0 Policy Audit

6.1 Secure Care UK (Secure Care) fully accepts the obligations placed upon it by the various Acts of Parliament and its contracts and responsibilities. A programme of audits will be undertaken to include (but not limited to):

• A Data Quality Audit • An archiving compliance audit • A review of the register of systems • An annual audit of staff training along with an survey of staff opinions on data security in line with the latest questions in the NHS Data Protection and Security Toolkit recommendations	• A Data Protection Impact Assessment Compliance Audit • Annual Systems Stress Test including a review of anti virus and security outputs • The quality of information in the annual submission of the NHS Data Protection and Security Toolkit • Audit of data disposals contractor
---	---

7.0 Data protection principles

7.1 Secure Care UK is committed to processing data in accordance with its responsibilities under the GDPR. Article 5 of the GDPR requires that personal data shall be:

- a. processed lawfully, fairly and in a transparent manner in relation to individuals;
- b. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
- c. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- d. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
- e. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and
- f. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss,

destruction or damage, using appropriate technical or organisational measures.

- g. When Secure Care UK enters into a substantial new client relationship or implements a new system the Finance and IT Manager acting as the Data Protection Officer and SIRO shall conduct and act upon a Data Protection Impact Assessment (Appendix 1)
- h. The organisation will follow NHS guidance and undertake Cyber essentials

7.2 General provisions

- a. This policy applies to all personal data processed by the organisation.
- b. The Finance and IT Manager shall take responsibility for the organisation's ongoing compliance with this policy as the organisations nominated Data Protection Officer.
- c. Secure Care UK shall register with the Information Commissioner's Office as an organisation that processes personal data.

7.3. Lawful, fair and transparent processing

- a. To ensure its processing of data is lawful, fair and transparent, the organisation shall maintain a Register of Systems.
- b. The Register of Systems shall be reviewed at least annually.
- c. Individuals have the right to access their personal data and any such requests made to the organisation shall be dealt with in a timely manner and as per the commitments made in the organisations Data Transparency Statement (See Appendix 2).

7.4. Lawful purposes

- a. All data processed by the organisation must be done on one of the following lawful bases: consent, contract, legal obligation, vital interests, public task or legitimate interests ([see ICO guidance for more information](#)).
- b. The Organisation shall note the appropriate lawful basis in the Register of Systems.
- c. Where consent is relied upon as a lawful basis for processing data, evidence of opt-in consent shall be kept with the personal data.
- d. Where communications are sent to individuals based on their consent, the option for the individual to revoke their consent should be clearly available and systems should be in place to ensure such revocation is reflected accurately in Secure Care's systems.

7.5. Data minimisation

- a. Secure Care shall ensure that personal data are adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- b. The Organisation will adopt the principle of pseudonymisation when dealing with personal data and will ordinarily utilise the initials of an individual e.g. John Smith would become "JS".

7.6. Accuracy

- a. The organisation shall take reasonable steps to ensure personal data is accurate.

- b. Where necessary for the lawful basis on which data is processed, steps shall be put in place to ensure that personal data is kept up to date.
- a. To ensure that personal data is kept for no longer than necessary, the organisation shall put in place an archiving standard for each area in which personal data is processed and review this process annually.
- b. The archiving standard shall consider what data should/must be retained, for how long, and why and is shown below:

Data Type	Retention Period	Exceptions	Exceptions to be agreed by
Booking forms and patient risk assessments.	6 months	Any open investigations	Quality Manager
Records of employees who have left the organisation	7 years	Open legal cases	Managing Director
Invoices, remittance advices and expense claims	1 year	Open legal cases	Finance and IT Manager
Patient Care Records	1 year	Any Open investigations	Quality Manager
Patient opinion surveys	1 year		
Vehicle and asset check documents	2 years		

7.8. Security

- a. The organisation shall ensure that personal data is stored securely using modern software that is kept-up-to-date.
- b. The organisation shall ensure that up to date anti virus and general security protections are deployed
- c. Access to personal data shall be limited to personnel who need access and appropriate security should be in place to avoid unauthorised sharing of information.
- d. When personal data is deleted this should be done safely such that the data is irrecoverable.
- e. Appropriate back-up and disaster recovery solutions shall be in place.
- f. An annual stress test of systems shall be undertaken
- g. The Finance and IT Manager will maintain a register of all systems and include within this any areas where the latest releases of software are not in use and any High Risk data.
- h. All members of staff shall be trained to at least level 1 data security with an annual refresher

to be recorded through the eLearning portal.

- i. The organisation will follow NHS guidance and undertake Cyber Essentials certification
- j.

7.9. Breach

a. In the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, the organisation shall promptly assess the risk to people's rights and freedoms and if appropriate report this breach to the ICO ([more information on the ICO website](#)).

b. The Finance and IT manager in his/her role as SIRO will maintain a record of any data protection breaches.

8 Information Security Principles

8.1 This section outlines the approach, methodology and responsibilities for preserving the confidentiality, integrity and availability of Secure Care UK information. It is the overarching policy for information security and supported by specific technical security, operational security and security management policies. It supports the 7 Caldicott principles compliance with the NHS Information Governance Toolkit.

Caldicott
1. Justify the purpose(s) 2. Don't use personal confidential data unless it is absolutely necessary 3. Use the minimum necessary personal confidential data 4. Access to personal confidential data should be on a strict need-to-know basis 5. Everyone with access to personal confidential data should be aware of their responsibilities 6. Comply with the law 7. The duty to share information can be as important as the duty to protect patient confidentiality

8.2 The core information security principles are to protect the following information/data asset properties:

- Confidentiality (C) – protect information/data from breaches, unauthorised disclosures, loss of or unauthorised viewing.
- Integrity (I) – retain the integrity of the information/data by not allowing it to be modified.
- Availability (A) – maintain the availability of the information/data by protecting it from disruption and denial of service attacks.

In addition to the core principles of C, I and A, information security also relates to the protection of reputation; reputational loss can occur when any of the C, I or A properties are breached. The aggregation effect, by association or volume of data, can also impact upon the Confidentiality property.

For Secure Care UK the core principles are impacted, and the effect aggregated, when any data breach relates to patient care data.

8.3 Governance – Roles and Responsibilities

a. All Staff

Information Security and the appropriate protection of information assets is the responsibility of all users and individuals are expected at all times to act in a professional and responsible manner whilst conducting Secure Care UK's business. All staff are responsible for information security and remain accountable for their actions in relation to Secure Care and other UK Government information and information systems. Staff **shall** ensure that they understand their role and responsibilities, and that failure to comply with this policy may result in disciplinary action. This will be reinforced by yearly mandatory training.

b. Finance and IT Manager

The Finance and IT Manager shall act as the Senior Information Risk Owner (SIRO) and is accountable for information risk within Secure Care and advises the Board on the effectiveness of information risk management across the organisation. The Finance and IT Manager will also undertake the role of Data Protection Officer and is responsible for ensuring implementation of this policy Data Security Standards with respect to Patient Confidential Data. (S)he

- Communicate and promote awareness of the Act across Securecare
- Lead on matters concerning individuals right to access information held Secure Care and the transparency agenda.

c. Support from Clinical Advisor

It is recognised that the services provided by Secure Care UK are clinical in nature and that the advice of a qualified and registered clinician is important particularly when advising the Managing Director in his/her role as Caldicott Guardian. The Chairman of the board will make arrangements to ensure that the board has a suitably qualified clinician as an advisor.

d. Senior Responsible Owners

All Senior Managers, Heads of Department, Information Risk Owners and Directors, defined as Senior Responsible Owners (SROs), are individually responsible for ensuring that this policy and information security principles **shall** be implemented, managed and maintained in their business area. This includes:

- Awareness of information security risks, threats and possible vulnerabilities within the business area and complying with relevant policies and procedures to monitor and manage such risks
- Supporting personal accountability of users within the business area(s) for Information Security
- Ensuring that all staff under their management have access to the information required to perform their job function within the boundaries of this policy and associated policies and procedures.

8.4 Compliance Requirements

a.Audit

Audit will be performed as part of the ongoing Secure Care Audit Programme and the Information Security Officer shall ensure appropriate evidence and records are provided to support these activities at least on an annual basis. The Quality Manager is accountable to the Governance Committee and the board to ensure this programme is undertaken

b.Review

This policy shall be reviewed at least annually by the reviewers noted within the Reviewers section of this policy. The Finance and IT Manager shall be responsible for ensuring the review is conducted in good order and follows due process for approval.

The Finance and IT Manager is accountable for providing the results of ongoing reviews of information security implementation across Secure Care. This includes support to the annual Information Governance Toolkit return.

c.Records Management

Records management is vital to the delivery of our services in an orderly, efficient, and accountable manner. Effective records management will help ensure that we have the right information at the right time to make the right decisions. It will provide evidence of what we do and why, therefore protecting the interests of the Commissioner, his staff and all who interact with the Information Commissioner's Office (ICO). Records, and the information they preserve, are an important corporate asset.

We aim to balance our commitment to openness and transparency with our responsibility for patient and employee confidentiality. So we will create and manage records efficiently, make them accessible where possible, protect and store them securely and dispose of them safely at the right time.

By adopting this policy we aim to ensure that the record, whatever form it takes, is accurate, reliable, ordered, complete, useful, up to date and accessible whenever it is needed to:

- help us carry out our business
- help us to make informed decisions;
- protect the rights of employees,
- regulated entities, and the public;
- track policy changes and development;
- make sure we comply with relevant legislation;
- provide an audit trail to meet business, regulatory and legal requirements;
- make sure that we work effectively as a regulator and prosecuting authority and meet our lawful obligations for disclosing evidence;
- support continuity and consistency in management and administration
- make sure we are open, transparent and responsive
- support research and development
- promote our achievements.

8 Freedom of information Act

8.1 The Freedom of Information Act 2000 (the Act) provides a right of public access to information held by organisations providing services to public bodies. Secure Care UK is committed to its obligations under the Act which require it to do the following:

- Publish certain information about its activities
- Respond to requests for information

8.2 Under the terms of the Act individuals may submit written requests for information to the organisation and these will be accepted via email as described in our Data Transparency Statement

8.3 Requestors have a right to be informed within 20 working days whether the organisation holds the requested information and if so, subject to paragraph 8.4 to receive a copy of the information.

8.4 There are [23 exemptions](#) under the Act which entitle Secure Care UK to withhold information if it considers it is appropriate to do so. If the decision is made to withhold the information it will provide the requestor with the following:

- Confirmation, if appropriate, whether the requested information is held
- Details of the appropriate exemption under the Act
- Reasons why it considers the exemption applies
- Details of the review procedure.

8.5 Information which can be complied accurately within 2-3 hours will normally be provided free of charge.

8.6 Secure Care UK complies with the Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations (2004). All requests that take less than 2-3 hours or £100 (being the “appropriate limit”) to process will be free of charge. If the estimated time for compliance is in excess of 3 hours then the organisation may refuse the request or alternatively may issue

an invoice for the estimated cost, such invoice to be paid before the organisation undertakes its retrieval of the requested information.

9 Internal Review and Complaints

9.1 Requestors have the right to ask for an internal review of how their request has been handled. This includes where the requested information has been withheld.

9.2 Such requests should be submitted in writing to info@securecareuk.co.uk

9.3 The internal review will be carried out by the Managing Director within 20 working days of receipt.

9.4 If the requestor is dissatisfied with the outcome of the internal review then they can appeal the decision to the Information Commissioner's Office (ICO) which oversees compliance with the Act. The ICO can be contacted at the following address:

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF.
Telephone 0303 1231113.
Email: casework@ico.org.uk

Appendix 1 – Data Protection Impact Assessment Screening Checklist



Data Protection Impact Assessment
Screening Checklist

SECURE CARE UK
SECURE PATIENT TRANSPORT SPECIALISTS



New Process or Relationship:

Overview:

Should a Data Protection Impact Assessment be Carried out?

- ☐ We consider carrying out a DPIA in any major project involving the use of personal data.
- ☐ We consider whether to do a DPIA if we plan to carry out any other:
 - ☐ evaluation or scoring;
 - ☐ automated decision-making with significant effects;
 - ☐ systematic monitoring;
 - ☐ processing of sensitive data or data of a highly personal nature;
 - ☐ processing on a large scale;
 - ☐ processing of data concerning vulnerable data subjects;
 - ☐ innovative technological or organisational solutions;

- ☐ processing that involves preventing data subjects from exercising a right or using a service or contract.
- ☐ We always carry out a DPIA if we plan to:
 - ☐ use systematic and extensive profiling or automated decision-making to make significant decisions about people;
 - ☐ process special-category data or criminal-offence data on a large scale;
 - ☐ systematically monitor a publicly accessible place on a large scale;
 - ☐ use innovative technology in combination with any of the criteria in the European guidelines;
 - ☐ use profiling, automated decision-making or special category data to help make decisions on someone's access to a service, opportunity or benefit;
 - ☐ carry out profiling on a large scale;
 - ☐ process biometric or genetic data in combination with any of the criteria in the European guidelines;
 - ☐ combine, compare or match data from multiple sources;
 - ☐ process personal data without providing a privacy notice directly to the individual in combination with any of the criteria in the European guidelines;
 - ☐ process personal data in a way that involves tracking individuals' online or offline location or behaviour, in combination with any of the criteria in the European guidelines;
 - ☐ process children's personal data for profiling or automated decision-making or for marketing purposes, or offer online services directly to them;
 - ☐ process personal data that could result in a risk of physical harm in the event of a security breach.
- ☐ We carry out a new DPIA if there is a change to the nature, scope, context or purposes of our processing.
- ☐ If we decide not to carry out a DPIA, we document our reasons.

Should a Data Protection Impact Analysis be conducted? Yes or No (please circle)

Reason for decision:

If Yes continue below.

In No

Data Protection Impact Analysis Steps

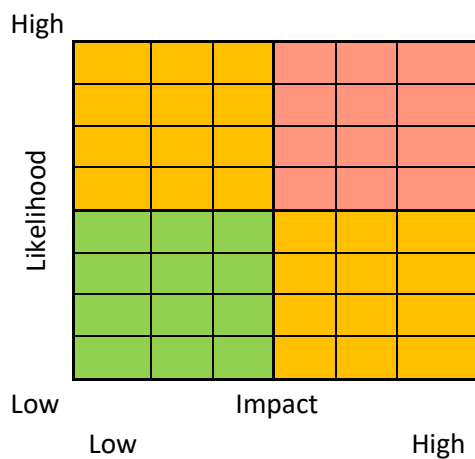


Describe the data processing which will occur

Is there a need to consult with clients or patient groups? Considering necessity and proportionality

What are the risks and what would be the impact/likelihood of any issues?

Please place a "X" in one square. (One table for each risk)



What Contingencies and Mitigations are to be implemented as a result of this assessment?

No	Action	Who	By when or complete

Formally accepted by Governance Committee on:

Formally accepted by Board on:

Full Implementation check diarised for:

Full Implementation signed off by..... On

Appendix 2– Data Transparency Statement

SECURE CARE UK
SECURE PATIENT TRANSPORT SPECIALISTS



Data Transparency Statement

SECURE CARE UK
SECURE PATIENT TRANSPORT SPECIALISTS



Your rights

Data protection laws in the UK give people a number of rights concerning their personal data. Not all rights apply equally to all our processing activity as certain rights are not available depending on the lawful basis for the processing. These rights are:

1. [Right to be informed](#)
2. [Right of access](#)
3. [Right to rectification](#)
4. [Right to erasure](#)
5. [Right to restrict processing](#)
6. [Right to data portability](#)
7. [Right to object](#)
8. [Rights in relation to automated decision making and profiling.](#)

We want you to feel confident that we look after everyone's personal data in line with the law. If you have any questions about your rights, you can get in touch with us at info@securecareuk.co.uk

Requesting a copy of your information

Typically, we collect information from health and care organisations providing your care and would advise contacting them directly for a more complete record of your care or treatment. We do not hold your whole medical or care record.

If you would like to request a copy of your personal data that Secure Care UK is processing then you will need to complete a subject access request. Please email info@securecareuk.co.uk and place "Subject Access Request" in the title of the email.

Following your request, we may write back to you within the 30-day timeframe to request you to narrow or modify your requirements. This may also result in an extension of a further 40 days whilst we examine your request. Some information requests may fall under the Freedom of Information Act in which case if the request is significant it may be appropriate to charge for the time to complete the report.

Sharing information

There are very strict rules about who can access the personal data we process, and what it can be used for. When information is shared with other organisations, these organisations have to go through an audit and have a clear data management agreement in place with ourselves.

Where necessary Secure Care UK will undertake a Data Protection Impact Assessment prior to the commencement of any new major system project or any substantial new business relationship or contract.

Copies of Data Protection Impact Assessments can be requested by way of an email to infor@securecareuk.co.uk

Data retention

All data is retained and erased in accordance with our Record Management Schedule. Specific retention periods are identified within each processing purpose listed below. If a specific purpose requires a different retention period outside of our policy this will be explained.

Complaints

If you wish to raise a complaint concerning NHS Digital's processing activity, visit our [Feedback and Complaints](#) page. You also have the right to raise a concern with the [Information commissioner's Office](#) at any time.