Data Security and Protection Policy

Version 4

Author:	Jenny Webster		
Approved By:	Dr Laura Neilson	Date: March 2020	Review Date: March 2021

Introduction: Information Security Policy for Focused Care CIC

1. Policy introduction & purpose

The Focused Care CIC Data Security and Protection Policy refers to our commitment to treat information of employees, customers, stakeholders and other interested parties with the utmost care and confidentiality.

With this policy, we ensure that we gather, store and handle data fairly, transparently and with respect towards individual rights.

This policy shall apply to information, systems, networks, applications, locations and staff of Focused Care CIC. It is based on the expectations set out within the Information Security Management: Code of Practice for NHS organisations, The Data Protection Act 2018, and The General Data Protection Regulations 2018.

The purpose of this policy is to enable and maintain effective security and confidentiality of information processed or stored by the Focused Care practitioners and wider staff. This shall be achieved by:

- Ensuring that all members of staff are aware of and shall comply with relevant legislation, including the Data Protection Act (1998) and the Data Protection (Processing of Sensitive Personal Data) Order 2000, and the General Data Protection Regulations 2018.
- Describing the principles of information security management and describing how they shall be implemented within Focused Care CIC
- Introducing an approach to information security that is consistent with other NHS organisations.
- Assisting staff to identify and implement information security as an integral part of their day to day role within the practice.
- Safeguarding information relating to staff and patients under the control of the practice.
- Describing the guidelines and procedures for reporting and dealing with breaches in the policy and handling of incidents.

This policy is split into two parts covering the updated national GDPR 2018 guidelines and the second covering NHS Information Guidelines for workers in the healthcare system.

2. Objectives

Key objectives of this Information Security Policy are to preserve:

- **Confidentiality** - Access to information shall be restricted to those with agreed authority to view it.
- **Integrity** – Records are to be complete and accurate with all filing and management systems operating correctly.
- **Availability** - Information shall be readily available and delivered to the authorised medical professional, when it is needed.

3. Scope

This policy refers to all parties (employees, job candidates, customers, suppliers, patients, GP Surgeries etc.) who provide any amount of information to us.

4. Who is covered under the Data Protection Policy?

Employees of our company and its subsidiaries must follow this policy. Contractors, consultants, partners and any other external entities are also covered.

Our policy refers to anyone we collaborate with or acts on our behalf and may need occasional access to data.

5. Registration information and nominated persons

Dr Laura Neilson is the Senior Information Risk Officer (SIRO):

The key responsibilities of the lead are:

- To develop an Information Governance Policy with assistance from the NHS England and the relevant CCG areas and /or maintain the currency of the policy;
- To ensure that the approach to information handling is communicated to all staff and made available to the public;
- To coordinate the activities of staff given data protection, confidentiality, information quality, records management and Freedom of Information responsibilities;
- To be Caldicott Lead for the practice ensuring that patient data is kept secure and that all data flows, internal and external are periodically checked against the Caldicott principles;
- To monitor the Practice's information handling activities to ensure compliance with law and guidance;
- To ensure that training made available is taken up by staff as necessary to support their role.

The day to day responsibilities for guidance to staff would be undertaken by the **Information Governance Lead and Data Protection Officer Focused Care Co-ordinator, Jenny Webster.**

NHS Data Security and Protection Toolkit . This online toolkit outlines the requirements for compliance with NHS Standards and must be completed annually. The final report is published and available for public reading via the website.

For the purposes of the Toolkit **Jenny Webster is the Information Governance Lead**, and responsible for the upkeep of this website and the evidence required within it. Focused Care CIC is subscribed to toolkit under the Organisation code 8JY14.

The Caldicott Principles 2013 are guidelines for handling personal and sensitive data in the NHS. Each NHS organisation must appoint a Caldicott Guardian to support the company in protecting data, and if shared, to share data appropriately.

Dr John Patterson is the Clinical Director and Caldicott Guardian for Focused Care CIC.

Information Commissioners Office (ICO)
The ICO is the UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals.

ICO Organisation name: Focused Care CIC
Reference Number: ZA439776
Data Protection Officer: Jenny Webster
Renewal Date: 08.07.2020

6. Policy elements

As part of our operations, we need to obtain and process information. This information includes any offline or online data that makes a person identifiable such as names, addresses, usernames and passwords, digital footprints, photographs, social security numbers, financial data etc.

As a company which operates as an Employer and a provider of medical services there are several areas to consider in order to meet data protection requirements.

For the purpose of this policy the principal areas of focus are as follows:

- Employee information – what information is kept, how it is kept, and how it may be used by the company or accessed by staff
- Patient information – day to day working with patients – gaining consent to use patient information, keeping caselists, referrals, and appointments etc.
- GP Surgery information – contact lists, correspondence
- Information for Evaluation and research purposes.

Our company collects this information in a transparent way and only with the full cooperation and knowledge of interested parties.

7. Responsibilities for Information Security

- Responsibility for information security shall rest with the Senior Information Risk Officer and Caldicott Guardian. However, on a day-to-day basis the Focused Care Co-ordinator, in partnership with local general practices in which Focused Care operates, shall be responsible for organising, implementing and managing this policy and its related good working practices.
- The Focused Care Co-ordinator shall be responsible for ensuring that both permanent and temporary staff including any contractors are aware of:-
  - The information security policies applicable to their work areas
  - Their personal responsibilities for information security
  - Who to ask or approach for further advice on information security matters.

- All staff shall abide by security procedures as set out by Focused Care CIC. This shall include the maintenance of all records whilst ensuring that their confidentiality and integrity are not breached (this applies to patient, staff and practice information). Failure to do so may result in disciplinary action.
- This Information Security Policy document shall be owned, maintained, reviewed and updated by the Focused Care Co-ordinator and the Operations Team. This review shall take place annually. The results of which shall be made known to each practitioner.
- The staff shall be responsible for both the security of their immediate working environments and for security of information systems they use (e.g. workstations)
- Any contracts with third party organisations that allow access to the information systems shall be in place before access is allowed. These contracts shall ensure that the staff or sub-contractors of those external organisations shall comply with all the appropriate security policies / guidance required by the company.

8. Data Protection by Design

The GDPR requires organisations to put in place appropriate technical and organisational measures to implement the data protection principles and safeguard individual rights. This is 'data protection by design and by default'. This is now a legal requirement.
Data protection by design is about considering data protection and privacy issues upfront in everything we do. It can help you ensure that we comply with the GDPR's fundamental principles and requirements, and forms part of the focus on accountability.

As outlined on the ICO website to this end Focused Care works in the following way:

☐ We consider data protection issues as part of the design and implementation of systems, services, products and business practices.
☐ We make data protection an essential component of the core functionality of our processing systems and services.
☐ We anticipate risks and privacy-invasive events before they occur, and take steps to prevent harm to individuals.
☐ We only process the personal data that we need for our purposes(s), and that we only use the data for those purposes.
☐ We ensure that personal data is automatically protected in any IT system, service, product, and/or business practice, so that individuals should not have to take any specific action to protect their privacy.
☐ We provide the identity and contact information of those responsible for data protection both within our organisation and to individuals.
☐ We adopt a 'plain language' policy for any public documents so that individuals easily understand what we are doing with their personal data.
☐ We provide individuals with tools so they can determine how we are using their personal data, and whether our policies are being properly enforced.
☐ We offer strong privacy defaults, user-friendly options and controls, and respect user preferences.
☐ We only use data processors that provide sufficient guarantees of their technical and organisational measures for data protection by design.

☐ When we use other systems, services or products in our processing activities, we make sure that we only use those whose designers and manufacturers take data protection issues into account.
☐ We use privacy-enhancing technologies (PETs) to assist us in complying with our data protection by design obligations.
☐We do not request or store patient identifiable data when it is not absolutely necessary for patient care. All patient data which is used for evaluation or review outside of the company is anonymised or pseudonymised appropriately in accordance with the Legal Basis for Processing. Further guidance in relation to pseudonymisation and Anonymisation can be found in the ICO Document: https://ico.org.uk/media/for-organisations/documents/1061/anonymisation-code.pdf

9. Data Protection Impact Assessments (Guidance adapted from ICO website)

A Data Protection Impact Assessment (DPIA) is a process to help identify and minimise the data protection risks of a project. **DPIA are completed for processing that is** likely to result in a high risk **to individuals.** This includes some specified types of processing. We will refer to the ICO Checklist in order to determine if a DPIA is necessary.
It is also good practice to do a DPIA for any other major project which requires the processing of personal data.

A DPIA must:
- describe the nature, scope, context and purposes of the processing;
- assess necessity, proportionality and compliance measures;
- identify and assess risks to individuals; and
- identify any additional measures to mitigate those risks.

To assess the level of risk, we consider both the likelihood and the severity of any impact on individuals. High risk could result from either a high probability of some harm, or a lower possibility of serious harm.

The data protection officer is consulted and, where appropriate, individuals and relevant experts. Any processors may also need to assist you.
If we identify a high risk that you cannot mitigate, we will consult the ICO before starting the processing.
If we are processing for law-enforcement purposes, the DPIA process will work alongside the Guide to Law Enforcement Processing. If submission is required The ICO will give written advice within eight weeks, or 14 weeks in complex cases. If appropriate, the ICO may issue a formal warning not to process the data, or ban the processing altogether.

Focused Care will refer to the ICO Checklist available at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/

We also use the ICO provided DPIA Template to assist correct completion and implementation of the document.

Part 1 Outline GDPR requirements from the Information Commissioners Office (ICO)

10. Staff and Human Resources data

As an employer Focused Care CIC must hold some personal data in order to correctly and fairly complete the recruitment and employment process.

Once this information is available to us, the following rules apply:

Our data will be:

- Accurate and kept up-to-date.
- Collected fairly and for lawful purposes only.
- Processed by the company within its legal and moral boundaries
- Protected against any unauthorized or illegal access by internal or external parties
- Disposed of securely and in a timely manner

Our data will not be:

- Communicated informally
- Stored for more than a specified amount of time
- Transferred to organizations, states or countries that do not have adequate data protection policies
- Distributed to any party other than the ones agreed upon by the data's owner (exempting legitimate requests from law enforcement authorities)

In addition to ways of handling the data the company has direct obligations towards people to whom the data belongs.

Specifically we must:

- Let people know which of their data is collected. Inform people about how we'll process their data Inform people about who has access to their information
- Have provisions in cases of lost, corrupted or compromised data
- Allow people to request that we modify, erase, reduce or correct data contained in our databases

Actions

To exercise data protection we're committed to:

- Restrict and monitor access to sensitive data
- Develop transparent data collection procedures
- Train employees in online privacy and security measures
- Build secure networks to protect online data from cyberattacks

- Establish clear procedures for reporting privacy breaches or data misuse
- Include contract clauses or communicate statements on how we handle data
- Establish data protection practices (document shredding, secure locks, data encryption, frequent backups, access authorization etc.)
- Our data protection provisions will appear on our website.

All guidance for staff in relation to the above is included in the Staff Privacy Notice which is distributed at the time of employment, and available at all times via the company online HR Toolkit.

Policy on reporting and recording a data breach is included in this policy under Section 13:

11. Disciplinary Consequences

All principles described in this policy must be strictly followed. A breach of data protection guidelines will invoke disciplinary and possibly legal action.

12. Key definitions for Data handling and protection: (From ICO Website)

Those involved in handling data or having their data being processed have been given the following titles according to the ICO website;

i. Data Controller:

A controller determines the purposes and means of processing personal data.

However, if you are a controller, you are not relieved of your obligations where a processor is involved – the GDPR places further obligations on you to ensure your contracts with processors comply with the GDPR.

ii. Data Processor:

A processor is responsible for processing personal data on behalf of a controller.

If you are a processor, the GDPR places specific legal obligations on you; for example, you are required to maintain records of personal data and processing activities. You will have legal liability if you are responsible for a breach.

iii. Data Subject:

The “Data Subject” is the person about who the data is held.

13. Data Subject Rights

The GDPR provides the following rights for individuals:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling.

All data subjects are asked to complete a consent form and given information in the relevant Privacy Notice which is also available on the company website and/or internal systems.

14. Data subject request for information

- Should a data subject wish to request to see information held about them they should complete a **Subject Access Request Form** and submit it to the Data Protection Officer.
- Data will be provided in electronic form.
- Data requested will be responded to within 40 days of receipt of the request.
- There will be no monetary charge to the data subject for this information
- All data requests received will be kept on the Focused Care **Subject Access Request Register** and the register will be reviewed on an annual basis.

15. National Data Opt-out Policy

Focused Care is compliant with the national data opt-out policy. Patients are made aware of the option to opt-out of data usage, which is also explained in the Focused Care Patient Privacy Notice. Signed consent for use of patient data is required at this stage and patients are able to revoke their consent at any time and do so b contacting their Focused Care Practitioner, or the Data Protection Officer based at the main office.

In the vast majority of cases any data used is anonymised in accordance with ICO guidelines. However, When Focused Care is required to process patient identifiable information such as NHS numbers, these are run through the check for national data opt-outs-service before being submitted, and any numbers where patients have opted out will be removed. Policy and directions for the completion of this task can be found via the links below:

Compliance with National Data Opt-outs
https://digital.nhs.uk/data-and-information/information-standards/information-standards-and-data-collections-including-extractions/publications-and-notifications/standards-and-collections/dcb3058-compliance-with-national-data-opt-outs

Check for national data opt-outs service
https://digital.nhs.uk/services/national-data-opt-out/compliance-with-the-national-data-opt-out/check-for-national-data-opt-outs-service

16. Reporting a breach of data regulations

Should an employee, contractor or patient of Focused Care CIC find that a breach of regulations has occurred they must report it to the Data Protection Officer immediately. The Data Protection must then report a genuine data breach to the Information Commissioners Office using their usual channels via the website: https://ico.org.uk/for-organisations/report-a-breach/

Any reported data breaches will be logged in the company **Data Breach Register**. This register will be reviewed on an annual basis

The person reporting the breach (or the DPO) will complete and fill out a Focused Care Significant Event Analysis in order to support any investigation and consider any learning from the incident. This form is available on the company internal systems or by request from the Focused Care office.

17. Staff Training

Staff training will take place on an annual basis after review of this policy, or at relevant times such as when policy is updated.

On induction staff will undergo training on Data protection and confidentiality
Staff will be asked to complete a **Training Needs Analysis Survey** in relation to Data Security and Protection on an annual basis

Staff will also be required to complete the online training modules to support their learning and understanding.

- Accessible Information Standard
- Consent
- Information Governance
- Records Management
- Risk Management

The Information Governance Lead will monitor staff compliance with the above policy.

Part 2 : Focused Care Information Governance Policy

2.1 Summary and introduction

This part of the policy relates to NHS and health guidelines for staff and employees in the use of health and company information. It goes hand in hand with the GDPR section of this policy.

Information is a vital asset, both in terms of the clinical management of individual patients and the efficient management of services and resources. It plays a key part in clinical governance, service planning and performance management.

It is therefore of paramount importance to ensure that information is efficiently managed, and that appropriate policies, procedures and management accountability and structures provide a robust governance framework for information management.

2.2 Principles

Focused Care CIC recognises the need for an appropriate balance between openness and confidentiality in the management and use of information. Focused Care CIC fully supports the principles of corporate governance and recognises its public accountability, but equally places importance on the confidentiality of, and the security arrangements to safeguard, both personal information about patients and staff and commercially sensitive information. Focused Care CIC also recognises the need to share patient information with other health organisations and other agencies in a controlled manner consistent with the interests of the patient and, in some circumstances, the public interest.

Focused Care CIC believes that accurate, timely and relevant information is essential to deliver the highest quality health care. As such it is the responsibility of everyone in Focused Care CIC to ensure and promote the quality of information and to actively use information in decision making processes.

There are 4 key interlinked strands to the information governance policy:

- Openness
- Legal compliance
- Information security
- Quality assurance

2.3 Openness

- Non-confidential information about Focused Care CIC and its services should be available to the public through a variety of media, in line with Focused Care CIC's code of openness
- Focused Care CIC will establish and maintain policies to ensure compliance with the Freedom of Information Act

- Focused Care CIC will undertake or commission annual assessments and audits of its policies and arrangements for openness
- Patients should have ready access to information relating to their own health care, their options for treatment and their rights as patients
- Focused Care CIC will have clear procedures and arrangements for liaison with the press and broadcasting media
- Focused Care CIC will have clear procedures and arrangements for handling queries from patients and the public

2.4 Legal Compliance

- Focused Care CIC regards all person identifiable information, including that relating to patients, as confidential
- Focused Care CIC will undertake or commission annual assessments and audits of its compliance with legal requirements
- Focused Care CIC regards all identifiable personal information relating to staff as confidential except where national policy on accountability and openness requires otherwise
- Focused Care CIC will establish and maintain policies to ensure compliance with the Data Protection Act, Human Rights Act and the common law confidentiality
- Focused Care CIC will establish and maintain policies for the controlled and appropriate sharing of patient information with other agencies, taking account of relevant legislation (e.g. Health and Social Care Act, Crime and Disorder Act, Protection of Children Act)

iv. 2.5 Information Security

- Focused Care CIC will establish and maintain policies for the effective and secure management of its information assets and resources
- Focused Care CIC will undertake or commission annual assessments and audits of its information and IT security arrangements
- Focused Care CIC will promote effective confidentiality and security practice to its staff through policies, procedures and training
- Focused Care CIC will establish and maintain incident reporting procedures and will monitor and investigate all reported instances of actual or potential breaches of confidentiality and security

2.6 Information Quality Assurance

- Focused Care CIC will establish and maintain policies and procedures for information quality assurance and the effective management of records
- Focused Care CIC will undertake or commission annual assessments and audits of its information quality and records management arrangements
- Managers are expected to take ownership of, and seek to improve, the quality of information within their services

- Wherever possible, information quality should be assured at the point of collection
- Focused Care CIC will promote information quality and effective records management through policies, procedures/user manuals and training

2.7 Responsibilities

The designated Information Governance Lead in the company is the Focused Care Co-ordinator, although staff should also be aware of the Information Governance Lead at the practices from which they work. The Focused Care Co-ordinator is responsible for overseeing day to day Information Governance issues; developing and maintaining policies, standards, procedures and guidance, coordinating Information Governance in the practice, raising awareness of Information Governance and ensuring that there is ongoing compliance with the policy and its supporting standards and guidelines.

All staff, whether permanent, temporary or contracted, are responsible for ensuring that they remain aware of the requirements incumbent upon them for ensuring compliance on a day to day basis.

2.8 Policy Approval

Focused Care CIC 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 of its stakeholders.

This policy, and its supporting standards and work instruction, look to support and compliment the individual practices Information Governance Policy.

We will, therefore, ensure that all staff, contractors and other relevant parties observe the policy under which the practice runs while working from that building, in order to ensure compliance with Information Governance and contribute to the achievement of the Focused Care CIC objectives and delivery of effective healthcare to the local population.

2.9 The Focused Care CIC shall undertake to ensure:

v. **Contracts of Employment –** address information security requirements at the recruitment stage and that all contracts of employment shall contain a confidentiality clause. The information security requirements shall be included within job descriptions.

vi. **Access Controls –** that the practitioner will be aware and follow the access control policy of the practice with whom they are working with, and operate within these boundaries.

vii. **Equipment Security –** is effective in order to minimise losses, or damage to the Company. All information assets and equipment shall, where possible be physically protected from security threats and environmental hazards. (Locked

cabinets (fire proof if possible), clear desk policy and the limitation of risks in the surrounding work area etc).

viii. **Information Risk Assessment –** a regular assessment of the working environment shall be conducted to identify potential risks to the security of information. Where risks are identified, these should be noted and where possible mitigating action taken.

ix. **Security Incidents and weaknesses -** are to be recorded and reported to the Focused Care Co-ordinator and then to the Caldicott Guardian so that they can be investigated to establish their cause, impact and the effect on the Practice and its patients. (NB. remedial changes arising may need to be included within future staff working procedures, updates to policies and contracts of employment).The Practice with whom the security incident took place will be fully informed and involved in this process.

a. Should a data breach be confirmed a Data Breach it is the duty of the Data Protection Officer to report this to the ICO with immediate effect.

b. All data breaches will be recorded for learning purposes and kept on file in the Company Data Breach Register and reviewed on an annual basis.

x. **Protection from Malicious Software –** should be provided through the use of commercial strength anti-virus/anti-malware software. Where there is an internet connection an appropriate firewall shall be installed and managed. No new software shall be downloaded or installed on computer systems of the Practice without the explicit permission of the Practice Manager, and in some cases the GMSS team. Breach of this requirement may be subject to disciplinary action.

xi. **Secure Communications –** should be in place to ensure that all correspondence, faxes, email, telephone messages and transfer of patient records are conducted in a secure and confidential manner. The communication of NHS Confidential or NHS restricted information by email must be appropriately protected, using cryptographic controls (AES 256 bit or equivalent). NHSMail administered by the company is covered in the *Focused Care Acceptable Use and NHSMail Policy*

xii. **Business Continuity and Disaster Recovery Plans –** are in place so that in the event of a disruption to the information services of the Company, it is possible to activate relevant business contingency plans until affected services are restored.

xiii. Focused Care will not use **unsupported systems** unless it is absolutely necessary to do so and the risk of doing so will be treated or tolerated.

3. Further requirements:

i. Requirement 10-116 Staff Confidentiality Agreement

All staff when they join the practice are asked to sign the companies Staff Confidentiality Agreement. The agreement forms part of their contract with Focused Care CIC.

In addition, all staff receive a copy of the staff handbook, which goes into more depth of the expectations of staff in regards to Information Governance.

All external staff are required to sign our confidentiality agreement when they begin work with us or have access to areas of the building where they may have access to I.T systems or patient information. These signed agreements are then stored by the Focused Care Co-ordinator. They are valid for one year.

All staff will be routinely monitored in regards to their compliance with the Information Governance and Security policies of Focused Care CIC.

All incidents, where staff have not complied with the Information Governance and Security policies, will be treated as potential 'gross misconduct' and disciplinary procedure may be started with that member of staff.

ii. Requirement 10-117 Staff training

Each job role with Focused Care CIC will have an assigned Information Governance and Security training plan which must be completed by all staff. The training plans are determined by which modules are relevant to their job roles. The formal training takes place online and is the official NHS Information Governance training tool.

The Focused Care Co-ordinator is responsible for ensuring that all staff have completed the required training.

Information Governance and Security training is part of the initial training for all new starters. They will be given basic training during their first two weeks in relation to Focused Care CIC's policies and procedures.
The formal online training will be required to be completed within the first two months employment with the company. Time will be allocated for this to happen.

Updates to training will be done annually or sooner if the Co-ordinator feels the staff member needs additional training. A checklist (appendix 2) of updated training will form part of the staff member's annual appraisal,

Compliance checks and routine monitoring is undertaken to test staff understanding and to ensure procedures are being complied with, where necessary, actions are taken.

iii. Requirement 10-211 Access to premises and sharing of information

The areas where personal or sensitive information is sent and/or received within the practice, it must be kept secure and confidential and free from public access.

All staff have a duty to ensure that the unauthorised access to personal or sensitive information in the following areas is maintained.

- Reception Area
- Clinical Rooms
- Admin Office
- Patient Records Storage Room

- Fax Machine
- Email
- Clinical System
- Printers

To aid this the Focused Care office is only accessible via PIN Code from public areas, Personal information and data is kept in locked cupboards and all devices are password protected.

All staff and visitors are required to sign in and out of the building in order to aid tracking of movements, and CCTV is also installed throughout the premises. Windows are locked when the office is empty.

Focused Care CIC follows the Caldicott Principles when transferring patient identifiable information.

Principle 1 Justify the purpose for using confidential information
Principle 2 Only use identifiable information if absolutely necessary
Principle 3 Use the minimum that is required
Principle 4 Access should be on a strict need to know basis
Principle 5 Everyone must understand their responsibilities
Principle 6 Understand and comply with the law

iv. Requirement 10-212 Gaining consent

Gaining patient consent is an integral part of patient / health professional relationship. All Focused Care practitioners obtain a written consent form from the patient before commencing working with them. At all levels of decision making, including referrals and assistance offered, verbal consent is obtained before any action commences.

v. Requirement 10-213 Duty to patients – privacy notices

Due to the nature of what we do, we have access to personal and sensitive information about our patients. It is important that our patients know how we collect information, why we need it and who has access to it.

It is the responsibility of all staff to ensure that:

Information about the personal data we store and the way we collect, store and delete is within our privacy notices. The leaflet is available from our website and is available to all patients.

Vi Requirement 10-304 NHS Smart Card Use

All Focused Care practitioners and support staff that work within practices are issued an NHS Smart Card. The smart card enables them to access Choose and Book, issue Electronic Prescriptions and have access to the NHS Demographic Service.

All staff who are issued with a smart card are required to keep the smart card safe and adhere to the national NHS smart card policies and procedures.
Staff should not

- Leave their card in the computer overnight or when they leave for a period of time (e.g. Lunch)
- Let others use their card or give out password

When a member of staff leaves the practice they can either

- Keep their smart card if they are moving to another NHS organisation
- Or hand it to the Focused Care Co-ordinator or Sponsor if they are leaving the NHS

If the staff member hands the card back, the Focused Care Co-ordinator or Sponsor must inform the Registration Authority of this and hand the card to them.

Each Practice Manager will be the site 'Sponsor' unless the card has been sponsored by the Focused Care Coordinator.

vii. Requirement 10-316 Information Asset Register

An information asset register is compiled by the company which shows what I.T hardware and software is held at each site. All I.T equipment and software is owned and maintained by the company. This asset register is stored in the company Data Security and GDPR files and a hard copy kept with the Business Continuity Plan.

Viii Requirement 10-317 Room and buildings access and data security

All staff at Focused Care CIC have a duty to protect our buildings and stored data from being accessed by unauthorised people.

Some examples are

- Locking rooms that are not being used
- Making sure the building is properly secured and alarmed at the end of the day

- Logging off computers when the staff member leaves their desk
- Not leaving patients notes and letters on desks or in view of the public

Iix. Requirement 10-318 Use of mobile devices

Additional security measures and care must be taken when using mobile devices which store personal information which are taken out of the practice.

Steps must be taken to make sure that only the authorised staff member has access to the device and it is stored securely when not being used.

No identifiable information is stored on the app, which is used to gather data around the households visited and to assist caseload management.

ix. Requirement 10-319 Business Continuity Plan

A documented Business Continuity Plan is available to staff in order to deal with any disruption to core services which may happen unexpectedly.

The plan will show how the plan will be activated, who to contact in emergency, alternative locations in case the practice cannot be used.

The plan is reviewed and tested annually by each practice.

x. Requirement 10-320 IT faults or Data Breaches

All faults and problems with the I.T equipment and software is reported to central office.

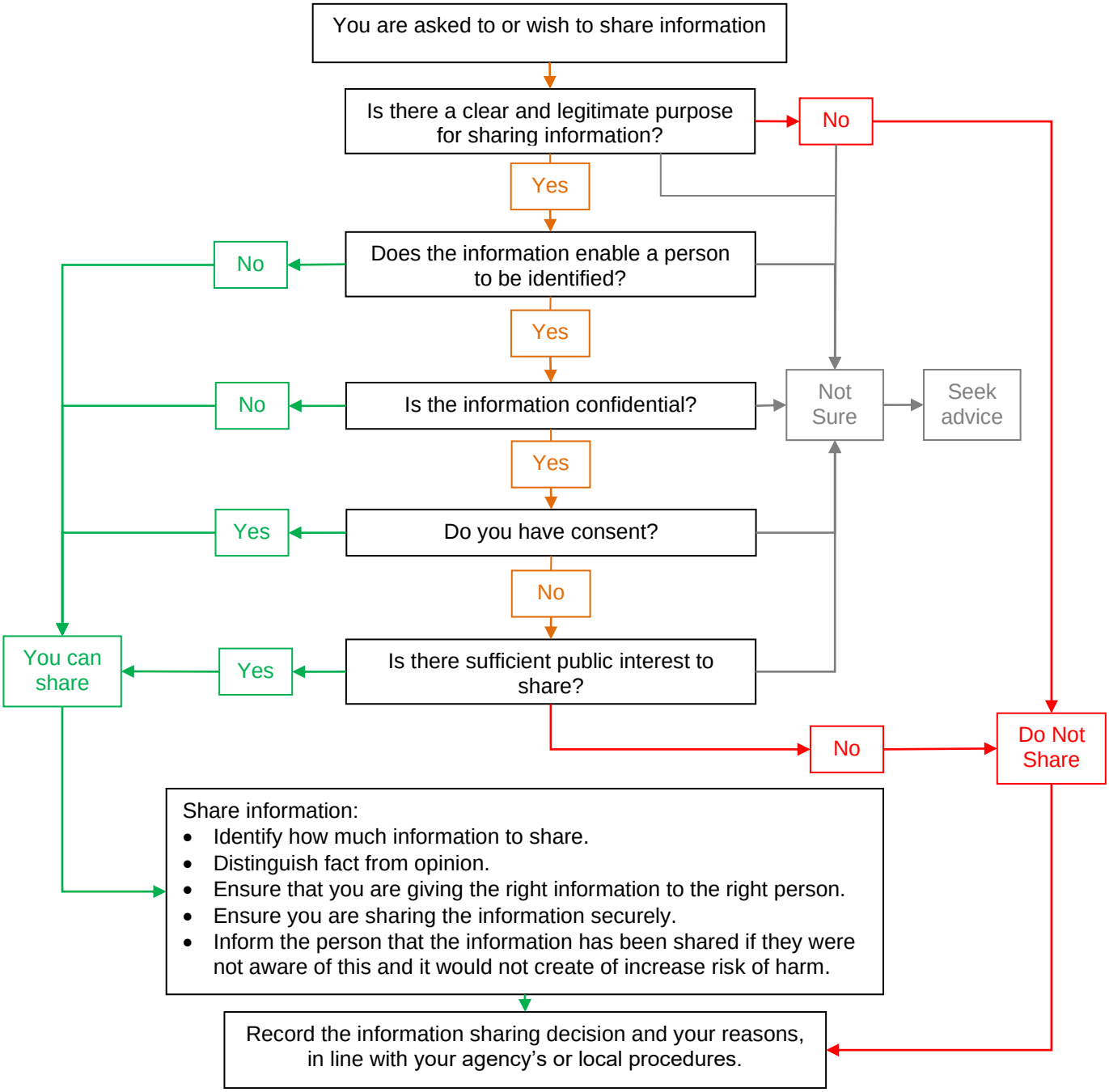
All information security incidents, near-misses and breaches are reported through the Focused Care CIC significant event process. This will allow the incident, near-miss or breach to be reported, investigated, learnt from and audited.

Any serious incidents must be reported to the Data Protection Officer (Jenny Webster), Caldicott Guardian (Dr John Patterson) or a member of the Operations team if either of the above are not available as soon after the incident as possible.

The associated documents to each requirement can be found at the bottom of this document or within one of the other CQC policies.

Appendix 1: Information Sharing Guidance And Seven Golden Rules

FLOWCHART FOR KEY QUESTIONS FOR INFORMATION SHARING



If there are concerns that a child may be at risk of significant harm or an adult may be at risk of serious harm, then follow the relevant procedures without delay.
Seek advice if you are not sure what to do at any stage and ensure that the outcome of the discussion is recorded.

Appendix 2

Company Policies:
Staff Handbook
Confidentiality Policy,
Data Protection and Information Governance Policy

Further reading and external links:
Data Protection Act of 2018 (UK)
General Data Protection Regulations 2018
Information Security Management: Code of Practice for NHS organisations.
Data protection in United States

Caldicott Principles: https://www.igt.hscic.gov.uk/Caldicott2Principles.aspx

Physical Asset Register for data storage

PLEASE SEE FOCUSED CARE DATA SYSTEMS ASSET REGISTER FOR FURTHER INFO.

Please also see **Focused Care Phone and Tablet Log** for further information in relation to company devices. All phones and tablets are encrypted and require a passcode to access