

# Cranes Park Road Surgery

## DATA SECURITY AND PROTECTION POLICY

### Document History

Document Reference:	IG01
Document Purpose:	This policy sets out the practice Cranes Park Road Surgery expect from all staff, including those working on behalf of the Practice, when complying with Data Protection legislation within the practice.
Date Approved:	20/11/2018
Version Number:	1.0
Status:	FINAL
Next Revision Due:	November 2020
Developed by:	Paul Couldrey – IG Consultant
Policy Sponsor:	Richard Johnson, Practice Manager
Target Audience:	This policy applies to any person directly employed, contracted, working on behalf of the Practice or volunteering with the Practice.
Associated Documents:	All Information Governance Policies and the Information Governance Toolkit, and Data Security and Protections Toolkit 2018

## CONTENTS

Section	
1	Introduction
2	Policy Aims
3	Policy Scope
4	Definitions
5	Principles of DS&P Policy
6	Roles and Responsibilities
7	Policy Statements, Standards*, Processes*, Procedures* and Associated Documents
8	Patient Confidentiality
9	Education and Training Requirements
10	Process for Monitoring Compliance
11	Equality Impact Assessment
12	Legal Liability
13	Supporting References, Evidence Base and Related Policies
14	Process for Version Control, Document Archiving and Review
15	Development and Consultation

### **REVIEW DATES AND DETAILS OF CHANGES MADE DURING THE REVIEW**

---

This is a new policy developed to support the Information Governance Toolkit and from April 2018 the NHS Digital Data Security and Protections Assurance Toolkit

### **KEY WORDS**

---

Information governance, confidentiality, security, data protection, IG Toolkit, SIRO, Caldicott Guardian, Privacy, DS&P Toolkit

## **SUMMARY**

---

This document provides a policy statement on the use and management of information in the Practice and describes the arrangements for providing assurance to the Practice Management Team that IG compliance standards are defined and met and IG incidents appropriately managed.

## **1 INTRODUCTION**

---

The Data Protection Act 1998/ Data Protection Act 2018 (DPA) and the General Data Protection Regulation (GDPR) impose obligations on the use of all personal data held by Cranes Park Road Surgery whether it relates to patients and their families, employees, complainants, contractors or any other individual who comes into contact with the organisation. This has implications for every part of the organisation. The Practice also has a duty to comply with guidance issued by the Department of Health, the NHS Executive, NHS Digital and the NHS Information Governance Alliance the specific requirements of the Information Governance (IG) Toolkit Toolkit (from April 2018 the NHS Digital Data Security and Protections Assurance Toolkit) and guidance issued by professional bodies.

- 1.1 The Practice and its employees are bound by a legal duty of confidentiality to all patients which can only be set aside to meet an overriding public interest, legal obligation, or similar duty. The DPA and GDPR apply all staff, contractors and volunteers working for the Practice. Cranes Park Road Surgery is a Data Controller, as defined in Article 3 (7) of the GDPR and Section 1 of the DPA and is obliged to ensure that all the Data Protection requirements are implemented. The requirements of Article 5 (1) of the GDPR and be able to demonstrate compliance with those requirements Article 5(2).
- 1.2 This policy sets out how the Practice meets its legal obligations and requirements under confidentiality, Data Protection and information security standards. The chief requirements outlined in this Policy are based upon the DPA/GDPR, which is the central piece of legislation covering security and confidentiality of personal information.

## 2 POLICY AIMS

---

- 2.1 This Data Protection Policy (the Policy) aims to ensure that Cranes Park Road Surgery (the Practice) meets its legal obligations and NHS requirements concerning confidentiality and information security standards. The requirements within the Policy are primarily based upon the General Data Protection Regulation (GDPR) 2016 that is the key piece of legislation covering security and confidentiality of personal information.

## 3 POLICY SCOPE

---

- 3.1 This policy covers all forms of information held by the Practice, including (but not limited to):

- Information about members of the public
- Non-Practice employees on Practice premises
- Staff and Personnel information
- Organisational, business and operational information

This policy applies to all Practice employees and third parties responsible for the delivery of contracted NHS services on behalf of the organisation.

## 4 DEFINITIONS

---

- 4.1 **Information Governance (IG);** IG is the organisational practice of managing information from its creation to final disposal in compliance with all relevant information rights legislation. IG is focused on ensuring that standards and services are introduced to ensure that Practice information is managed securely, compliant with legislation and available for access by both staff and external parties, including the public and regulators.

- 4.2 **Information Governance Toolkit (IGT)/ Data Security and Protections Toolkit;** The assessment toolkits are supported by both NHS Digital and NHS England and are self-assessment tool for Practices which incorporates a knowledge base and guidance all aspects of IG. The IGT/DS&P is updated annually to reflect new NHS guidance, legislation and NHS Codes of Practice.

## 5

- 5.1 **Senior Information Risk Owner (SIRO);** The SIRO takes ownership of the practice's information risk policy and acts as an advocate for information risk on behalf of the Practice who is also the Senior Information Risk Officer. The SIRO for the Practice is the Richard Johnson.
- 5.2 **Caldicott Guardian;** The Practice's Caldicott Guardian has a particular responsibility for reflecting patients' interests regarding the use of patient identifiable information. They are responsible for ensuring patient identifiable information is shared in an appropriate and secure manner. The Caldicott Guardian is Dr. Mona Attalla.
- 5.3 **Data Controller;** means the natural or legal person, public authority (Cranes Park Road Surgery), agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law; Article 4(7) GDPR.

## 6 Principles of DPC Policy

---

- 6.1 To meet the vision for managing DPC standards there are three key interlinked aims to the policy which will ensure the delivery of an effective policy framework:
- **Legal compliance;** The Practice aims to meet and exceed all compliance requirements relating to DPC. The Practice will undertake or commission annual assessments and audits of its compliance with legal requirements through the Appropriate IG Toolkit and demonstrating compliance to all relevant healthcare standards, the policy will also demonstrate that the Practice has adopted the Accountability for demonstrating compliance with the GDPR as required by Article 5(2).
  - **Information security;** The Practice will promote effective confidentiality and security practice to its staff through an Information Security Management Systems (ISMS) which includes policies, procedures and training. The Practice has established and maintains incident reporting procedures and will monitor and investigate all reported instances of actual or potential breaches of confidentiality and security.
  - **Openness;** Non-confidential information on the Practice and its services should be available to the public through a variety of media. The Practice will undertake or commission annual assessments and audits of its policies and arrangements for openness through the IG Toolkit.
- 6.2 The Practice has developed the Data Protection and Confidentiality Policy to enable the delivery of these three key aims for this policy.

## 7 ROLES AND RESPONSIBILITIES

---

### Practice Management Team

- 7.1 The Practice Management Team has overall accountability for the Practice's ability to meet the policy requirements. The Management Team is responsible for:
- Receiving, considering and approving regular reports and briefings;
  - Signing off the Practice's Privacy Strategy and annual IG and DS&P toolkit returns.
- 7.2 On behalf of the Management Team, the Information Governance Steering Group is responsible, for ensuring adequate arrangements are in place.

### **Executive Lead**

- 7.3 The Senior Partner has overall responsibility for information governance in the Practice. As Accountable officer he/she is responsible for the management of information governance within the Practice and for ensuring appropriate mechanisms are in place to support service delivery and continuity. The Practice has a particular responsibility for ensuring that it corporately meets its legal responsibilities, and for the adoption of internal and external governance requirements.

### **Caldicott Guardian**

- 7.4 The Practice Caldicott Guardian has Management Team level responsibilities for the Practice's Caldicott Function and enables a direct reporting line to the Practice Management Team and the appropriate governance committee. The Caldicott Guardian is responsible for protecting the confidentiality of service user information and enabling lawful and ethical information sharing. This links directly to information governance (IG) and will require an IG Lead to liaise directly with the Caldicott Guardian.

### **Senior Information Risk Officer**

- 7.5 The Senior Information Risk Officer (SIRO) has Management Team level responsibilities and takes overall ownership of the Practice's IG processes and provides written advice to the Senior Partner on the content of the Practice's Annual Governance Statement in regard to information risk.

### **Information Governance Steering Group**

7.6 The Information Governance Steering Group is responsible on behalf of the Practice for;

- Developing, implementing and maintaining a ISMS and associated policies, an annual work programme to provide assurance to the Practice that effective arrangements are in place;
- Agreeing IG relevant reports and recommendations and timely preparation of the annual IG assessment for Practice Management Team sign off;
  
- Promote and embed IG into the organisational culture.

### **IG Lead – Practice Manager**

6.7 The nominated IG Lead is the Practice Manager (Richard Johnson). The IG Lead has responsibility for project managing the overall co-ordination, publicising and monitoring of the Practice IG Framework. The Practice IG Lead has specific responsibility for the development of this policy, producing performance monitoring reports and producing IG toolkit central returns on behalf of the Practice.

### **Data Protection Officer – PCIG Consulting Limited**

6.8 Paul Couldrey of PCIG Consulting Limited will act as the Data Protection Officer (DPO) for Practice, This role is key to ensuring that Practice comply and can demonstrate that they comply with the GDPR.

### **Practice Employees & staff working on behalf of the Practice**

6.9 All Practice employees, whether permanent, temporary or contracted, and students 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. All employees are required to undertake regular Practice mandatory training in IG to ensure that they are fully aware of their individual responsibilities and have the relevant knowledge to ensure compliance. Misuse of or a failure to properly safeguard information may be regarded as a disciplinary offence.



## **8 POLICY STATEMENTS**

---

- 8.1 When Practice staff manages any business information then s/he is required to comply with the requirements of the procedures and requirements. This policy requires all staff to manage information to the highest standards to ensure compliance with appropriate standards, to secure all Practice information and to promote appropriate information access.
- 8.2 The Practice fully endorses the six principles set out in the GDPR 2016. The Practice and all staff who process personal information must ensure these principles are followed. In summary these state that personal data shall: -
- (a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');
  - (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, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');
  - (c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');
  - (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 ('accuracy');
  - (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 in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');
  - (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 ('integrity and confidentiality').

- 8.3 Furthermore, the Practice is committed to implementing the seven Caldicott principles for handling patient-identifiable information, namely: -
- 1 Justify the purpose of using patient identifiable information.
  - 2 Only use patient identifiable information when absolutely necessary.
  - 3 Use the minimum necessary patient identifiable information.
  - 4 Access patient identifiable information on a strict need to know basis.
  - 5 Everyone should be aware of their responsibilities.
  - 6 Understand and comply with the law.
  - 7 The duty to share information can be as important as the duty to protect patient confidentiality

8.4 Any breach of the Data Protection legislation with specific reference to unauthorised use/disclosure of personal data or failure to safeguard personal data in accordance with Practice policy will be viewed as gross misconduct and may result in serious disciplinary action being taken, up to and including dismissal. Employees could also face criminal proceedings.

## **8.5 Subject Access**

There is a recognised procedure (The PATIENT ACCESS TO MEDICAL RECORDS POLICY & PROXY ACCESS 2018) by which personal data is disclosed either to the data subject or to their representative.

Any request must be completed within a maximum of one month from date or receipt, 25 May there will be no fee charged for SAR.

## **8.6 Confidentiality**

The 'Confidentiality: NHS Code of Practice' has been published by NHS England. The consultation included patients, carers and citizens; the NHS; other health care providers; professional bodies and regulators.

This document is a guide to required practice for those who work within or under contract to NHS organisations concerning confidentiality and patients' consent to the use of their health records.

## **8.0 PATIENT CONFIDENTIALITY**

---

- 8.1** Health information is collected from patients in confidence and attracts a common law duty of confidence until it has been effectively anonymised. This legal duty prohibits information use and disclosure without consent – effectively providing individuals with a degree of control over who sees information they provide in confidence. This duty can only be overridden if there is a statutory requirement, a court order, or if there is a robust public interest justification.
- 8.2** On first contact with the Practice, all patients should be asked which relatives, friends or carers they wish to receive information regarding treatment and progress, or those they specifically do not give permission to receive information.
- 8.3** In cases where relatives have been heavily involved in patient care, the patient must be explicitly asked as to what level these relatives can be kept informed. This is particularly important in cases where relatives are requesting information on the patient's condition, perhaps before the patient has been informed.
- 8.4** In the event a person lacks capacity to consent to information being shared staff should check if a person is authorised by a Lasting Power of Attorney (health and welfare) or been appointed by the court of protection to make that decision. The document must be seen. This person can consent on their behalf but must act in the person's best interest. If they have not, then no one can consent on behalf of that person. A professional in the care team must assess if it is in the best interest of the person to share the information. The person's wishes and feeling, although not determinative, should be the starting point in this assessment.

## **Staff Confidentiality**

- 8.5** All Staff are required to keep confidential any information regarding patients and staff, only informing those that have a need to know. In particular, telephone conversations and electronic communications must be conducted in a confidential manner.
- 8.6** Confidential information must not be disclosed to unauthorised parties without prior authorisation by a senior manager. Staff must not process any personal information in contravention of the GDPR 2016 or DPA2018.
- 8.7** Any breaches of these requirements will potentially be regarded as serious misconduct and as such may result in disciplinary action.
- 8.8** All staff have a confidentiality clause in their contract of employment. The practice has an approved Data Protection and Confidentiality clause in all contracts with 3rd party contractors and suppliers who process personal information.

## **9 EDUCATION AND TRAINING REQUIREMENTS**

---

- 9.1** The Practice is committed to the provision of IG training and education to ensure the workforce is informed, competent, prepared and possesses the necessary skills and knowledge to perform and respond appropriately to the demands of clinical care and service delivery.
- 9.2** The Practice has a mandatory training programme which includes maintaining awareness of IG, data protection, confidentiality and security issues for all staff. This is carried out by regular training sessions covering the following subjects:
- personal responsibilities;
  - confidentiality of personal information;
  - relevant IG Policies and Procedures;
  - general good practice guidelines covering security and confidentiality;
  - records management.
- 9.3** All staff will be required to complete annual IG training (including data protection and confidentiality training) commensurate with their duties and responsibilities. All new starters will be given IG training as part of the Practice mandatory induction process.

## **10 PROCESS FOR MONITORING COMPLIANCE**

---

- 10.1 The IG Lead will establish a performance management framework, reported through the Information Governance Steering Group on a six monthly basis.

## **11 EQUALITY IMPACT ASSESSMENT**

---

- 11.1 The Practice recognises the diversity of the local community it serves. Our aim therefore is to provide a safe environment free from discrimination and treat all individuals fairly with dignity and appropriately according to their needs.
- 11.2 As part of its development, this policy and its impact on equality have been reviewed and no detriment was identified.

## **12 LEGAL LIABILITY**

---

- 12.1 The Practice will generally assume vicarious liability for the acts of its staff, including those on honorary contract. However, it is incumbent on staff to ensure that they;
- Have undergone any suitable training identified as necessary under the terms of this policy or otherwise.
  - Have been fully authorised by their line manager to undertake the activity.
  - Fully comply with the terms of any relevant Practice policies and/or procedures at all times.
  - Only depart from any relevant Practice guidelines providing always that such departure is confined to the specific needs of individual circumstances. In healthcare delivery such departure shall only be undertaken where, in the judgement of the responsible clinician it is fully appropriate and justifiable – such decision to be fully recorded in the patient's notes.
- 12.2 Staff contracts of employment are produced and monitored by the Practice. All contracts of employment include a data protection and general confidentiality clause as part of controls to enhance privacy and information governance. Agency and contract staff are subject to the same rules.

## 13 SUPPORTING REFERENCES, EVIDENCE BASE AND RELATED POLICIES

---

13.1 The Senior Information Risk Owner (SIRO) will direct the IG Lead to take actions as necessary to comply with the legal and professional obligations set out in the key national guidance issued by appropriate commissioning bodies in particular;

- [The NHS Confidentiality Code of Practice](#)
- [Care Record Guarantee](#)
- [NHS Records Management Code of Practice Part 2](#)
- [NHS IGA GDPR Guidance](#)
- [Information Security Management: NHS Code of Practice](#)

13.2 There are a number of policies and procedures within the Practice that should be read in conjunction with this document for a complete understanding of how the Practice is organised and the strategies in place to fulfil its obligations. The key documents are listed below:

- Patient Access to Medical Records Policy and Proxy Access 2018
- Practice Responsibilities Document
- Records Policy
- Breach Reporting Policy

#### **14 Due Regard**

This policy has been reviewed in relation to having due regard to the Public-Sector Equality Duty (PSED) of the Equality Act 2010 to eliminate discrimination, harassment, victimisation; to advance equality of opportunity; and foster good relations.

#### **15 Review and Monitoring**

The Practice Manager is responsible for regular monitoring of the quality of records and documentation and managers should periodically undertake quality control checks to ensure that the standards as detailed in this policy are maintained.

This policy will be reviewed every two years unless new legislation, codes of practice or national standards are introduced.