The Jubilee Street Practice

Data Security and Protection Policy

Date of last review or update: 4th April 2019

Introduction

The Jubilee Street Practice (the practice) needs to have a Data Protection Policy to demonstrate compliance with the General Data Protection Regulation (GDPR) and UK Data Protection Legislation. This policy sets out the general arrangements by which we will be compliant under the various Articles of GDPR and UK Data Protection Act 2018.

The Data Controller details are below, and these can be found on the Information Commissioner's Office Data Protection register.

Data Controller: The partners of The Jubilee Street Practice, 368-374 Commercial Road, London, E1 0LS
Data Protection Registration Number: Z5754665

As a general practice providing services under an NHS contract we process personal and special category data relating to our staff and those we treat, registered patients and others, internally and with other organisations external to the practice. We also hold data on other types of customers, suppliers, business contacts and other people we have relationships with or may need to contact.

We are required by certain laws to disclose certain types of data to other organisations on a regular basis such as NHS Digital, Public Health England, NHS England, the Local Authority, or the Tower Hamlets Clinical Commissioning Group.

We are also required by certain laws to disclose certain types of data to other organisations on an event by event basis, such as CQC or the General Medical Council.

These processing activities, and others, are described in detail in the Practice Privacy Notice. This can be found here: http://www.jubileestreetpractice.nhs.uk/.

Why this policy exists

The practice recognises that with the advance of technology, and more complex ways to share and communicate digitally, the emphasis of data processing needs to be refocused to a default of protection and ensure disclosure is lawful, informed, controlled, and of benefit to the data subject.

The GDPR enables the Practice to build patient trust in how we collect and use personal data, and improve the way we provide services.

We are open about how we store and process personal data, and protect ourselves from the risks of a data breach.

General

This policy applies no matter how the data is stored; electronically, documents, images, on paper. To comply with the law, personal data must only be collected and used fairly, stored safely and not disclosed unlawfully.

Personal data must:

- Be processed fairly and lawfully, and transparently, in line with UK Data Protection Legislation and the Common Law Duty Confidentiality
- Be obtained only for specific, lawful purposes
- Be adequate, relevant and not excessive
- Be accurate and kept up to date Not be held for any longer than necessary
- Be processed in accordance with the rights of data subjects
- Be protected in appropriate ways

Policy scope

This policy applies to our whole practice team, clinical and non-clinical, and to everyone who works within the practice. This includes anyone who has agreed that they have a duty of confidence, and has access to the practice systems, and patient, staff and/or organisation-confidential or business sensitive information. This will include but not be limited to all employees of the Practice, partner organisations who access record systems, locums, students, researchers, interns, volunteers and contractors.

It applies to all the personal data that we process.

Responsibilities

Everyone who works for or with the practice has shared responsibility for ensuring data is collected, stored and handled appropriately. Each person that handles personal data in this organisation must ensure that it is handled and processed in line with this policy and data protection principles.

The Practice, who holds the NHS GP contract, is the data controller, and is therefore responsible for ensuring that it meets all its legal obligations.

The following specific duties and responsibilities apply within the practice:

- The Transformation Partner has overall responsibility for the Data Protection Policy.
- The Caldecott Guardian has responsibility for placing appropriate controls and procedures for monitoring access to any person identifiable data held by the Practice.

- The Information Governance (IG) Lead is responsible for providing advice, liaising with other organisations to process subject access requests, co-ordinating the release of the data and investigating complaints.
- The Transformation Partner is responsible for ensuring all staff are aware and comply with this policy.
- All of the practice team, including contractors, volunteers, interns, researchers and agency staff are responsible for person identifiable data that they record or process and are obliged to adhere to this policy.

The Data Protection Officer

The Practice is a Public Authority, as the services we provide are under an NHS Contract, therefore, the Practice has designated a Data Protection Officer who:

- Keeps the practice informed about current data protection responsibilities and risks and issues
- Provides advice to the data controller
- Assists the data controller to monitor and maintain and demonstrate compliance
- Advises on the need for Data Privacy Impact Assessments
- Acts as a point of contact for data subjects and the ICO
- Provides an independent view, based on knowledge of UK data protection legislation

The practice

- Ensures that the DPO can operate independently and without limitation •
- Involves the DPO in relevant issues
- Ensures staff are trained and aware of GDPR requirements
- Ensures that the opinion of the DPO is always given due weight
- Will not issue the DPO with any instructions or place any constraints relating to their DPO role
- Will allow data subjects to contact the DPO
- Will comprehensively record and thoroughly document any reasons for acting against the advice of their DPO

Designation of the DPO

The practice has designated the Data Protection Officer role in the role of Dr Salma Ahmed.

The DPO contact details are salma.ahmed@nhs.net or Dr Salma Ahmed, The Data Protection Officer, The Jubilee Street Practice, 368-374 Commercial Road, London E1 0LS.

Information Technology Systems

- The practice IT systems and support are provided via Tower Hamlets CSU (Commissioning Support Unit) and under national contracts with clinical system providers.
- The practice ensures systems, services and equipment used for storing data meet acceptable security standards.
- Regular checks and reviews are performed to ensure security hardware and software is functioning properly.
- The practice liaises with the CSU provided IT infrastructure support services
- The practice ensures that cyber security recommendations are implemented and deployed, and continual staff awareness is raised regarding cyber security
- The practice liaises with the DPO on any technical matters relating to the GDPR.

The General Data Protection Regulation (GDPR) 2018

The GDPR came into force on 25 May 2018. and the UK Data Protection Act 2018 came into force in 2018 as well.

Contracts and Service Level Agreements

The Practice must ensure that appropriate wording regarding compliance with the Data Protection Act (and GDPR) is covered in all contracts and service level agreements before these are signed or changes are agreed. Temporary staff, students, volunteers and contractors are required to sign a confidentiality agreement. Copies are available from within the individual staff digital contracts saved under R:\Practice\F84031\F84031-Management\Personnel\Staff.

Training

All staff must complete information governance training on an annual basis. Compliance is monitored, and a reminder sent to those members of staff whose training is about to, or has, expired.

Data Processing Register and Privacy Notice

A register of data processing activities undertaken by the practice, and any data processing agreements entered into are maintained in a register, which is regularly updated and reviewed. This includes ensuring the GDPR legal basis for processing data is identified.

The practice regularly reviews, and updates as required, the Practice Privacy Notice, which is published on its website.

Changes to systems and processes – Data Protection Impact Assessments

It is important that changes to services and systems and processing of person identifiable data are assessed to ensure that confidentiality, accessibility and integrity

of data are maintained. The practice liaises with its DPO to identify when a Data Protection Impact Assessment (DPIA) is required and ensures this is completed and approved before changes are introduced.

Accuracy of data

All practice staff are responsible for ensuring that:

- Their own personal data provided in relation to their employment is accurate and up to date
- Person identifiable data that they handle lawfully as part of their role is as accurate and up to date as possible, kept securely with restricted access, and not kept for longer than necessary.

Security of Data

All staff are responsible for ensuring that personal or sensitive data is held securely and that it is not disclosed to any unauthorised third party. Data that is disclosed inappropriately or accidentally must be reported using the practice incident reporting process.

All data breaches are logged in a breach register. To ascertain if a breach is reportable to the ICO, the practice liaises with the DPO. Any reportable breaches are reported to the ICO within 72 hours where possible.

All data breaches are examined, whether reportable or not, to ensure measures are put in place to prevent recurrence, to reduce risk, and to ensure lessons are learned.

Retention of data

The Data Protection Act requires that data is not held for longer than necessary. Staff are required to identify the retention periods for all personal data held by them and ensure that it is disposed of securely in accordance with retention and destruction guidelines included in the Information Governance Alliance: Records Management Code of Practice for Health and Social Care 2016 https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-informationgovernance/information-governance-alliance-iga

Disclosure outside of the UK

Personal data, even if it would otherwise constitute fair processing, must not, unless certain exemptions apply, or protective measures are taken, be disclosed or transferred outside the UK to a country or territory which does not ensure an adequate level of protection for the rights and freedoms of data subjects. Advice should be sought from the Information Governance Lead/Data Protection Officer or Caldecott Guardian before any such information is transferred.

General staff guidelines

- The practice provides **training** to all employees to help them understand their responsibilities when handling data

- Staff should keep all data secure, by taking sensible precautions and following the practices procedures and policies
- NHS smartcards, passwords and logins must be used whenever possible and they should **never** be shared or borrowed
- Whenever a screen is left, programs that handle patient data should be closed or locked
- Personal data should **not be disclosed to unauthorised people**, either within the company or externally
- Staff should request help from the Information Governance Lead or the Caldecott Guardian in the first instance if they are unsure about any aspect of data protection
- Staff may liaise with the DPO where required
- All staff have a "Computer Equipment and Data Protection" and a "Confidential Information" clause within their contracts.

Relevant Legislation and Statutory Best Practice

The **Common Law Duty of Confidentiality** is that if information is given in circumstances where it is expected that a duty of confidence applies, that information cannot normally be disclosed without the information provider's consent unless there is an over-riding public interest (e.g. public health) or legal duty to do so (e.g. detection or prevention of serious crime).

The **UK Data Protection Act – DPA (2018)** controls how an individual's personal information is used by organisations, businesses or the government. Organisations that process PID must register with the Information Commissioner's Office on an annual basis.

From 25 May 2018, the DPA was repealed by the **European Union General Data Protection Regulation (GDPR)**. The overall principles of the GDPR are for organisations to be fair and transparent about how they use individuals' personal information, and for individuals, where possible, to have more choice and control over how their personal information is used. GDPR builds on current law and best practice. GDPR requires that the practice identifies the legal basis for processing, managing and sharing patient information.

Data protection legislation applies only to living individuals, who have a right to access information that an organisation holds about them. Please see the practice's Subject Access Request policy for further information.

A duty of confidence still applies to deceased individuals' personal information. The **Access to Health Records Act (1990)** confers the right of access to records of deceased patients to executors or administrators of a deceased person's estate and requests for access are administered in a similar way to requests for access to records under data protection law.

Caldecott Principles

The practice adheres to the Caldecott Principles, as listed below.

1. **Justify the purpose(s)**
   Every proposed use or transfer of personal confidential data within or from an organisation should be clearly defined, scrutinised and documented, with continuing uses regularly reviewed, by an appropriate guardian.

2. **Don't use personal confidential data unless it is absolutely necessary**
   Personal confidential data items should not be included unless it is essential for the specified purpose(s) of that flow. The need for patients to be identified should be considered at each stage of satisfying the purpose(s).

3. **Use the minimum necessary personal confidential data**
   Where use of personal confidential data is considered to be essential, the inclusion of each individual item of data should be considered and justified so that the minimum amount of personal confidential data is transferred or accessible as is necessary for a given function to be carried out.

4. **Access to personal confidential data should be on a strict need-to-know basis**
   Only those individuals who need access to personal confidential data should have access to it, and they should only have access to the data items that they need to see. This may mean introducing access controls or splitting data flows where one data flow is used for several purposes.

5. **Everyone with access to personal confidential data should be aware of their responsibilities**
   Action should be taken to ensure that those handling personal confidential data — both clinical and non-clinical staff — are made fully aware of their responsibilities and obligations to respect patient confidentiality.

6. **Comply with the law**
   Every use of personal confidential data must be lawful. Someone in each organisation handling personal confidential data should be responsible for ensuring that the organisation complies with legal requirements.

7. **The duty to share information can be as important as the duty to protect patient confidentiality**
   Health and social care professionals should have the confidence to share information in the best interests of their patients within the framework set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies.

Updates to this policy

This policy will be reviewed and updated as and when UK Data Protection requirements are changed.