Cairn Medical Practice

Patient Data.
Data Protection and GDPR Compliance Statement

Version= 1.2 (May 2018)

Version History

Version ID	Date	Author
Draft 1.0	03 Apr 2018	P Munro
Version 1.1	22 May 2018	P Munro
Version 1.2	23 May 2018	P Munro

1 Data Protection

1.1 Data Protection Officer

Our Data Protection Officer is Mr P Munro, the Practice Manager. He is responsible for ensuring compliance with the law and reports directly to the chair of the partnership. The Health Board has its own Data Protection Officer responsible for ensuring that organisation's compliance with the law.

1.2 Data Control

The Practice and the Health Board are joint Data Controllers for your medical records. For the practice, ultimate responsibility for Data Control/release of data rests with the Chair of the Partners. The Health Board has its own Data Controller responsible for ensuring that organisation's data handling meets their own internal protocols.

2 What Data we Hold.

The staff at this practice record information about you and your health so that you can receive the right care and treatment. We need to record this information, together with the details of the care you receive, because it may be needed if we see you again or if problems are identified with a drug that you have been prescribed. The data that we record are Name, Address, telephone number(s) and email plus records of your GP/Nurse consultations, drugs prescribed and any correspondence sent/received about you to/from other healthcare professionals. This may include test results and discussions about any referrals to secondary care.

In addition to standard medical data, we may record your telephone call and retain the recording for a period of up to 60 days to facilitate complaint investigation. If we need to retain a recording for longer than 60 days then we will inform you.

Some consultations are recorded on video to allow our GP training supervisors to review the standard of consultations made by our trainee GPs. These video recordings are made only with your consent; they are kept for a year and then destroyed.

3 General Data Protection Regulations

3.1 Legal Basis for Holding and Processing Your Data

We need to collect and process your data to provide a robust health service to you and to protect the public health. Paragraph 35 of the GDPR stipulates that:

> *Personal data concerning health should include all data pertaining to the health status of a data subject which reveal information relating to the past, current or future physical or mental health status of the data subject. This includes information about the natural person collected in the course of the registration for, or the provision of, health care services as referred to in Directive 2011/24/EU of the European Parliament and of the Council (1) to that natural person; a number, symbol or particular assigned to a natural person to uniquely identify the natural person for health purposes; information derived from the testing or examination of a body part or bodily substance, including from genetic data and biological samples; and any information on, for example, a disease, disability, disease risk, medical history, clinical treatment or the physiological or biomedical state of the data subject independent of its source, for example from a physician or other health professional, a hospital, a medical device or an in vitro diagnostic test.*

We collect and process your data under Article 6 (Paragraph 1, (c, d & e))

Processing shall be lawful only if and to the extent that at least one of the following applies:

(c) processing is necessary for compliance with a legal obligation to which the controller is subject;

(d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;

(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

Data about your health and wellbeing is classed under Article 9 of the GDPR as 'Special Category' data and the law requires that we identify a reason for processing Special Category data (GDPR Article 9 (Paragraph 1). Our reasons for processing Special Category Data are GDPR Article 9, Paragraph 1, sub sections c, g, h,i and j)

(c) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;

(g) processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;

(h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;

(i) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;

(j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be propor-tionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

4 How We Use Your Data

4.1 General

In addition to looking after your health interests, we may use some information to help us to protect the health of the general public generally, to plan for the future, to train staff and to carry out medical and other health research for the benefit of everyone.

5 Sharing and Protecting your Data

5.1 Sharing Data

We will not pass on your details to any organisation that is not within the NHS or acting under contract to the NHS, except in an emergency where it is in your interest, or where it has been ***judged*** to be in your best interest (for example, you have an accident abroad and a foreign hospital needs your medical information),or where we are compelled to by law. Even within the NHS, communication of your data is not routine and will be on a strict ;'need to know' basis, for example a hospital referral or seeking advice from a specialist in order to offer you appropriate treatment.

5.2 Research

We are involved in research studies for which we use a data set that has been redacted to prevent you from being identified; we refer to this as 'anonymised' data. All directly identifiable details (name, address, post code, NHS number, full date of birth) are removed from the data file before they are collected for research, and an automatic program de-personalises any free text (non structured or coded data). Currently, we share anonymised data with 3 research systems, SPIRE, THIN and SHARE

5.3 THIN.

The THIN database is managed under contract by a company outside the NHS which does not have access to your personal details, only to anonymous medical records. The data are used for research into such topics as drug safety, effectiveness of drugs, disease patterns, prescribing patterns, health economics and public health. Many of these studies provide useful information to medical staff on diseases, the use of drugs or outcomes of disease or treatment.

Individual patients' records are added into a much larger anonymous database, containing records from millions of patients across the UK. The database to which we contribute anonymised records is known as The Health Improvement Network (THIN).

The studies may be performed by academic researchers or commercial companies. However, no researcher has access to your identifiable details. In addition, as a further safeguard, the researchers are not given information about the GP nor the practice name, address or post code.

In the interests of transparency, we do receive a payment-in-kind for contributing to THIN. Our remuneration is not financial but free training for our staff on using our clinical IT system.

If you would like to opt out of this data collection scheme, please let your doctor know and no data from your records will be collected for use in research. This will not affect your care in any way.

The data processing agreement with Cegedim is between National Services Scotland and Cegedim and not with the practice

A list of published research using the THIN database can be found at http://csdmruk.cegedim.com/THINBibliography.pdf or please contact Michelle Page on telephone number 0207 554 0663 or email michelle.page@thin-uk.com for a paper copy.

5.4 SPIRE.

We also contribute to SPIRE, the Scottish Primary Care Information Resource. However, SPIRE do not hold data in a database but extract data on a case by case basis.

Full details about SPIRE are available here: http://spire.scot/your-questions-answered/. Again, you can opt out of SPIRE.

5.5 SHARE

We provide data to SHARE only with patient consent (opt in). Full details are available on the SPIRE webiste http://spire.scot/your-questions-answered/

5.6 Albasoft.

Albasoft is contracted by NHS Highland to process quality and achievement data on behalf of the NHS.

5.7 GDPR Data Processing Agreements.

National Services Scotland holds the responsibility for the Data Processing Agreement with SPIRE. Cegedim (who provide our clinical system) have the agreement with Public Health (Scotland) for THIN.[(1)] The data processing agreement with Albasoft is between NHS Highland and Albasoft and not with the practice.

We are in the process of clarifying whether the Health Board or individual practices need to pursue a Data Processing Agreement with SHARE.

Notes:

[(1)] – To be confirmed

6 Protecting Your Data

6.1 Methods of Security

The Practice employs a combination of physical and electronic methods to ensure the security of your data, plus regular audits and random sampling of physical documentation. Any electronic data transmitted out with the practice is via secure N3 network, encrypted email or encrypted USB data stick. Paper notes are couriered via the NHS' own internal network.

7 Accessing Your Data

7.1 General

You are entitled to have access to your medical records by making a Subject Access Request; under the GDPR we are not entitled to charge you a fee for this. You are also entitled to have any errors corrected.

Access by a 3rd Party commercial organisation, whom you have authorised to have access to your medical records (for instance by providing written authorisation to a solicitor or Insurance Company) may be chargeable. Beware of the type of authorisation that you provide to Insurance companies as they are not entitled to your full medical record but should request a targeted Medical report under the Access to Medical records Act.

Large volumes of information will be provided ONLY on an encrypted USB data stick in pdf format. Paper records will not be sent by mail or by standard courier services. Small amounts of data – eg a sheet containing test results, may be handed to you by the GP but will be stamped as 'Uncontrolled Copy – given to Patient'.

8 Deleting Your Data

8.1 Right to be Forgotten

Article 17 of the GDPR contains a right for a subject to have their data deleted permanently; this is known as the right to be forgotten. However, the legal basis for collecting health data is not based upon consent and the data remains relevant to the public health and to your personal interests.

Therefore, in general, your health records will not be deleted. After you leave the practice, your records are held by National Services (Scotland) PSD in Aberdeen; PSD will retain the data until 'no longer necessary in relation to the purposes for which they were collected or otherwise processed'.

9 Loss of Data

9.1 Physical Intrusion into Building

9.1.1 Any break in, or attempted break in will be treated as a potential breach of data protection. Physical storage will be checked for signs of entry and a random sample of paper records will be made. If a breach is detected then a full audit will be made and the Data Controller will inform the ICO.

9.2 Electronic Attack (Hacking or Virus)

9.2.1 The practice uses anti-virus and Firewall software provided by the NHS and has strict access policies for IT. In addition, any action by staff that compromises the physical security of the system (eg plugging in an unauthorized device) will be treated as Misconduct and will result in disciplinary action. Any detection of a virus or an attempt to gain unauthorized access to the IT system will be reported to NHS IT services who will investigate.

10 Queries and Concerns

You have a right of access to your health records. If at any time you would like to know more, or have any concerns about how we use your information, you can speak to the Data Protection Officer on 01463 712233

NHS Highland's Data Protection Officer is:

Donald Peterkin
Interim Data Protection Officer
NHS Highland
2nd Floor, Robertson FM Building
New Craigs
INVERNESS
IV3 8NP