Stoke Gifford and Conygre Medical Centre

Privacy Notice

Version 6 dated Nov 19

Contents

1. References:

- Data Protection Act 1998
- General Data Protection Regulations 2018
- Clinical, NHS England Standard Personal Medical Services Agreement 2015/16 based on National Health Service Act 2006;
- Stoke Gifford and Conygre Medical Centre Staff Handbook
- [] Model Publication Scheme

2. Lawful reasons for processing. Medical records data is controlled by the practice in order to fulfil a legal obligation under section 6(1)f of the GDPR where the processing of personal data 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*. In some cases, the Practice will share data lawfully under section 6 (1)d when it is *necessary to protect the vital interests of the data subject or another person where the data subject is incapable of giving consent,* or under 6(1)c where it is *necessary for compliance with a legal obligation*.

Staff HR records are maintained in order to fulfil the employment contract that we have with individuals and to comply with legal obligations. Processing / controlling data *necessary for the performance of a contract with the data subject or to take steps preparatory to such a contract* is defined as a legal basis in 6(1)b of the GDPR.

The special category condition for processing for direct care is that processing is, *'necessary for the purposes of preventive or occupational medicine, for the assessment of your working capacity, for medical diagnosis, for the provision of health or social care or treatment, or the management of health or social care systems and services..' (Article 9(2)(h)).* This would include our compliance with the Health and Social Care Act 2012.

For medical research purposes, the lawful basis and special category condition are Article (6)(1)(e) *'…for the performance of a task carried out in the public interest…'* and Article 9(2)(j) *'… for research purposes..'*

3. Data Protection Officer. The Data Protection Officer for Stoke Gifford and Conygre Medical Centre is Mr Mike Tregaskis and can be contacted at m.tregaskis@nhs.net.

4. How we use your information

This privacy notice tells you what to expect when Stoke Gifford and Conygre Medical Centre collects personal information. It applies to information we collect about:

1. People who use our services and their medical records.
2. Who subscribe to our newsletter or request a publication from us.
3. Job applicants and our current and former employees.
4. Visitors to our websites.
5. Complainants and other individuals in relation to: services provided by the medical centre; data protection or freedom of information complaint or enquiry.

5. People who use our services and their records. The practice has a contract with NHS England to provide Primary Medical Services. This contract requires us to: keep adequate records of its attendance on and treatment of its Patients and to do so: on forms supplied to it for that purpose by the Board; or with the written consent of the Board, by way of computerised records, or in a combination of those two ways.

The General Medical Council Good Practice Guidance (2013) advises our documents (including clinical records) to formally record patient interactions must be clear, accurate and legible. Records should be made at the same time as the events being recording or as soon as possible afterwards.

5.1 Patient medical histories and related documents, test results. We must keep records that contain personal information about patients, colleagues or others securely, and in line with any data protection requirements. These clinical records should include:

- relevant clinical findings,
- the decisions made and actions agreed, and who is making the decisions and agreeing the actions,
- the information given to patients,
- any drugs prescribed or other investigation or treatment,
- who is making the record and when.

In maintaining these patient medical histories, records of consultation discussions will be recorded. The records may include related documents from third parties that are relevant to your care and test results. Letters that are sent to you or on your behalf are also stored on your record.

5.2 Medical record storage.

5.2.1 Paper records. Paper records are stored in locked cabinets or in locked rooms that are not accessible to the public. We have a 'clean desk' policy that states that medical records should not be left insecurely when not in use or under control of the user.

5.2.2 Electronic Records. We have a computerised clinical management system called EMIS. The EMIS system securely stores all computerised records. Any data that is received from external sources is saved to this Electronic Record with any paper copies securely shredded. All practice staff have access to this electronic record via personal login details which must be kept confidentially and securely.

The EMIS Health Clinical System is provided through the local NHS Commissioning Support Unit and connected via a secure NHS internet system. EMIS Health are compliant with the Health and Social Care Information Centre (HSCIC) guidelines and have relevant registrations that include: ISO9001 for quality management systems; ISO20000 for IT service management and ISO27001 for information security. EMIS can also be used with nhs.mail to send text messages to patients.

The secure NHS System is managed by NHS Digital and who assure organisations using our IT systems follow good practice and the law when it comes to looking after information. The practice must:

- complete the Information Governance (IG) toolkit process
- sign up to the IG assurance statement
- maintain high IG standards and make sure their providers and suppliers do too
- comply with requirements set out in the Information governance statement of compliance to use the N3 network national broadband network for the NHS

5.3 Transfer of records. When patients move practices, paper records are forwarded to the new practice via a secure delivery service that is managed by NHS Primary Care Support England (PCSE). Electronic records can be sent directly into our clinical system using the GP2GP service. GP2GP allows patients' electronic health records to be transferred directly, securely, and quickly between their old and new practices, when they change GPs. This improves patient care by making full and detailed medical records available to practices, for a new patient's first and later consultations. The process is managed by NHS Digital. On

receipt of the new patient's paper records, the information held is checked against the electronic record and data added as required to ensure a full and accurate record.

5.4 Record Sharing. Our contract with NHS England requires a level of data sharing.

5.4.1 Disclosures which are required by law or clinical audit requirements

In order to comply with its legal obligations this practice may send data to NHS Digital when directed by the Secretary of State for Health under the Health and Social Care Act 2012'; and 'This practice contributes to national clinical audits and will send the data which are required by NHS Digital when the law allows. This may include demographic data, such as date of birth, and information about your health which is recorded in coded form, for example, the clinical code for diabetes or high blood pressure.

5.4.2 Disclosures for medical research or health management purposes

This practice contributes to medical research and may send relevant information to medical research databases such as the Clinical Practice Research Datalink and QResearch or others – when the law allows.

5.4.3 Data Sharing Initiatives.

There are currently 3 data sharing initiatives aimed at improving the NHS' responsiveness to changing medical care demand while aiming to improve the care that you receive by sharing medical information between certain NHS provider organisations. These are known as: the Summary Care Record; Care Data, and Connecting Care. They are all slightly different in aims and scope so please read the information below and follow the links for further details.

5.4.4 The Summary Care Record (SCR). The SCR is an electronic record which contains information about the medicines you take, allergies you suffer from and any bad reactions to medicines you have had. The aim of this data sharing is to allow clinicians from different settings to view key aspects of your record when providing care. E.g. in the event of an emergency. It can only be seen by healthcare staff involved in your care. You can opt out of this information sharing.

For more information see https://www.digital.nhs.uk/summary-care-records

5.4.5 NHS National Data. Whenever you use a health or care service, such as attending Accident & Emergency or using Community Care services, important information about you is collected in a patient record for that service. Collecting this information helps to ensure you get the best possible care and treatment. The information collected about you when you use these services can also be used and provided to other organisations for purposes beyond your individual care, for instance to help with:

- improving the quality and standards of care provided
- research into the development of new treatment
- preventing illness and diseases
- monitoring safety
- planning services
-

This may only take place when there is a clear legal basis to use this information. All these uses help to provide better health and care for you, your family and future generations. Confidential patient information about your health and care is only used like this where allowed by law. Most of the time, anonymised data is used for research and planning so that you cannot be identified in which case your confidential patient information isn't needed.

You have a choice about whether you want your confidential patient information to be used in this way. If you are happy with this use of information you do not need to do anything. If you do choose to opt out your confidential patient information will still be used to support your individual care.

To find out more or to register your choice to opt out, please visit www.nhs.uk/your-nhs-data-matters. On this web page you will:

- See what is meant by confidential patient information
- Find examples of when confidential patient information is used for individual care and examples of when it is used for purposes beyond individual care
- Find out more about the benefits of sharing data
- Understand more about who uses the data
- Find out how your data is protected
- Be able to access the system to view, set or change your opt-out setting
- Find the contact telephone number if you want to know any more or to set/change your opt-out by phone
- See the situations where the opt-out will not apply

You can also find out more about how patient information is used at:

https://www.hra.nhs.uk/information-about-patients/ (which covers health and care research); and

https://understandingpatientdata.org.uk/what-you-need-know (which covers how and why patient information is used, the safeguards and how decisions are made)

You can change your mind about your choice at any time. Please note, this opt out does not apply to local data sharing agreements that relate to data used to support an individual's care

5.4.6 Connecting Care. Connecting Care is a local electronic patient record that allows health and social care professionals directly involved in your care, to share a summary of your medical record. Your Connecting Care record will help those caring for you to manage your care better, and allow information to be shared quickly and safely. Only authorised staff providing health services across Bristol, South Gloucestershire and North Somerset can access your record.

For more information about Connecting Care, visit https://www.connectingcarebnssg.co.uk/. You will be asked for you consent to view your records and you can opt out of it.

5.4.7 Other instances occasioning third party access. We work with a number of organisations that have contracts with public bodies (such as the Local Authority, Public Health, Social Services, Clinical Commissioning Groups) to provide complementary services to our patients. This may include their conducting consultations with you or undertaking other activities that may require your data to be accessed. In such instances, data protection and confidentiality policies are in place and your permission will be sought prior to your record being accessed.

5.4.8 Other Data Sharing Requests. From time to time, local care providers will request access to anonymised data. Such requests are made in accordance with local NHS guidelines and agreement would be given following consideration by a GP Partner. We may also be asked to provide specific information about you following requests by other public bodies, e.g. Police, HM Courts, social services etc. Where such requests are made, any data provided is given in accordance with the guidelines laid down in the 1998 Data Protection Act. Namely that,

'1. personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless –

(a) at least one of the conditions in Schedule 2 is met, and

(b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.'

The Caldicott Principles for use of personal sensitive data are at Annex A.

5.4.9 Subject Access Requests (SARs) from Insurance Companies. Under the terms of the data protection act, we as the "data controller" have a responsibility to ensure the confidentiality and integrity of the information we hold about you. Furthermore, as your doctor we have a responsibility to ensure the confidentiality of matters of a sensitive medical, psychological, and emotional nature. A Subject Access Request requires us as data controller to give you as the "subject" access to all data we hold about you. This includes every recorded encounter you have had with any GP or nurse in the surgery as well as copies of all hospital letters, test results and prescriptions issued.

Insurance companies require medical information from yourself and ourselves to assess your risk of illness, death and disability. There is a system in place for GPs to give a pertinent summary of all relevant medical information (excluding information of a sensitive or irrelevant nature) by way of an industry approved General Practitioner's Report (GPR). The format of this report has been agreed by the Association of British Insurers and the British Medical Association. This system has been in place since then and a fee is paid by the insurance company to ourselves to ensure a prompt efficient service.

Lately some companies have been using the SAR system to obtain patients' full medical records. We have reason to believe that this may be done to reduce costs to the insurance company. More worryingly, we are concerned that our patients may not have received adequate explanation that their full record will be given to the insurance company, or that there is a simpler system in place whereby we can provide a GP report (or GPR) which releases only the relevant information.

Once we release a medical record to a third party we are no longer the data controller for that information, and we have no control over how that information is stored, used, or shared.

Due to concerns about how your data may be used, we no longer respond to Subject Access Requests by insurance companies. We will write to any requesting insurance companies to suggest that they submit a request to us for a GP report.

5.5 3rd party software, companies and Correspondence. In order to deliver the best possible service, the practice will share data (where required) with other NHS bodies such as other GP practices and hospitals. In addition the practice will use carefully selected third party service providers. When we use a third party service provider to process data on our behalf then we will always have an appropriate agreement in place to ensure that they keep the data secure, that they do not use or share information other than in accordance with our instructions and that they are operating appropriately. Examples of functions that may be carried out by third parties includes companies that provide IT services & support, including our core clinical systems; systems which manage patient facing services (such as our website and service accessible through the same); data hosting service providers; systems which facilitate appointment bookings or electronic

prescription services; document management services etc. Details regarding specific third party processors are as below and additional information can be supplied on request.

5.5.1 iGPR. Insurance companies use a firm called iGPR to request and receive insurance reports. We will only action these requests where the insurance company has provided us with signed consent from the patient. Niche Health's iGPR products are designed from inception to be fully compliant with best business and NHS security standards for the management of patient data. Niche Health is compliant with the NHS Information Governance (IG) Toolkit which ensures the safe handling and transmission of information for organisations working within the NHS environment. (http://www.nichehealth.co.uk/about/Information-Governance-And-Security.php)

5.5.2 MJOG. We use a text message reminder service to look ahead at our appointment book and send a text reminder about an appointment to a patient. We also use this service to send random Friends and Family Feedback questionnaires and reminders about health campaigns (e.g. quitting smoking service, NHS Health Checks or Flu jabs). These texts are all anonymous and sent to the mobile phone number that the patient would have provided. MJog employs stringent security measures to protect patient data and confidentiality and have an IGSoC rating of 100% and ISO27001:2013 certification. (https://www.mjog.com/healthcare/primary-care/).

5.5.3 Patient Chase. To help manage the care of our patients with chronic long term conditions, we use software called 'patient chase' to compile mail lists for specific groups of patients. PatientChase has several steps to ensure the correct security and information governance is maintained within the surgery.

What is stored

- Patient Demographics, QOF Searches and their connections are stored in the local PatientChase Database
- Saved searches store snapshots of searches with their associated datasets held in an a serialised dictionary
- Audited information around letters inserted into EMIS are stored in the shared database held in the local server

Encryption

- All searches, the local PatientChase Database and the shared database are encrypted (AES).
- 256-AES Encryption Algorithms are used
- No unencrypted data is stored on the client or server machine.

Other points

- The user has the option to store the PatientChase database on the local server for additional security.
- The shared PatientChase database is stored on the local server.
- When performing remote access to support and train our sights we use Logmein Rescue, known to several of the EMIS partners as the most secure way to communicate with the users using a secure 256 bit encrypted stream.
- No patient data ever leaves the surgery environment.

5.5.4 Docmail. Letters compiled by patient chase are sent to Docmail for printing and posting. All data is treated as confidential and Docmail will not use or disclose the data we send except as is necessary to complete the mailing. They will not release any of your information to a third party except where required

to by law, or, under certain circumstances, where that information is already in the public domain. Docmail utilise recognised 'best practice' security features to protect your data and maintain ISMS27001:2013 data security registration to ensure that this continues to be the case. No data is transferred outside of the European Economic Area except where permitted by Data Legislation. The data is only held for as long as is necessary to complete the mailing and they will delete all of the data you have provided to us after 30 days. Docmail maintain registration with the Data Protection Registrar and comply with the Data Protection Act 1998 in particular with the obligations set out in the seventh principle of Schedule 1 Part 2 of the Data Protection Act 1998.

5.5.5 Emails. Where possible, we will email you to inform you of any medical screening that you are due or to make you aware of relevant forthcoming health campaigns. Such emails are sent separately so your email addresses are not shared. Patients that have registered for the practice newsletter are sent these with addresses listed as Blind Carbon Copy (BCC). Where you ask us to send any of your records to you by email, we will send these securely and encrypted via our NHS secure email server. We will not email you data where we think there is a risk that the email may be accessible by others. Email addresses for the newsletters are stored on a secure server. Email addresses linked to patient records are stored on EMIS.

5.5.6 Fax. In order to avoid a fax containing patient or sensitive information being sent to the wrong person, breaching confidentiality and either delaying or denying the information to the intended recipient we will:

- Try to site fax machines away from public areas.
- Send faxes to named individuals if at all possible. Mark them 'addressee only'.
- Only send patient identifiable information by fax when absolutely necessary. Use identity numbers or initials if they will suffice.
- Not send more information than is required for the purpose and ensure that DPA principles are adhered to.
- Check the fax number is correct – use pre-programmed numbers where possible.
- Try to call the recipient to let them know the fax is about to be sent. Ask them to acknowledge receipt of the fax.
- Use a fax cover sheet that contains a confidentiality statement

'Safe Haven' fax machines: Where regular or semi-regular transmission of patient/staff sensitive information is going to take place by fax then 'safe havens' are used. A safe haven fax must be in a lockable environment (office or cupboard) where only those who need to see information sent have access and that when it is left unattended the facility is locked. Combining this increased physical security with the principles in the general guidance above will designate a fax as a 'safe haven'.

5.5.7 Shredding. All waste paper containing patient identifiable information is stored in locked bins and professionally shredded on-site and on a monthly basis by KN Office. Storage and shredding is managed securely in line with the Data Protection Act 1998. KN Office are fully compliant to BS EN15713.2008 and staff are vetted to BS7858 and CRB checked. The practice retains a Certificate of Destruction and Recycling Certificate.

5.5.8 Visitors to our websites. When someone visits www.stokegiffordmedical.co.uk we use a third party service, Google Analytics, to collect standard internet log information and details of visitor behaviour patterns. We do this to find out things such as the number of visitors to the various parts of the site. This information is only processed in a way which does not identify anyone. We do not make, and do not allow Google to make, any attempt to find out the identities of those visiting our website. If we do want to collect personally identifiable information through our website, we will be up front about this. We will make it clear when we collect personal information and will explain what we intend to do with it.

5.5.9 Search engine. Our website search is powered by GP Surgery.net. Their Privacy Statement can be found at https://gpsurgery.net/privacy/.

5.5.10. Ask My GP. Ask My GP askmyGP is an online consultation and workflow system that helps GPs manage patient caseload through operational change and digital triage. We make it easier for patients to talk to their own doctor and help GPs to prioritise and deliver care through message, phone and video. They are one of the on-line consultation providers that were recommended by the local NHS Clinical Commissioning Group and their privacy notice can be found at https://askmygp.uk/privacy-policy-gdpr/

5.6 Contacting us

5.6.1 Online contact page. Asked for clarifcaition of MSW

5.6.2 Telephone Calls. Our phone system is provided by Bistech. They provide itemised phone bills and allow us to record telephone calls for training and quality purposes. Bistech's management of data, associated to existing and prospective customers, is underpinned by the holding of both established BSI certifications to ISO 9001:2015 (Quality Management) and ISO 27001:2013 (Information Security Management) certifications, that combine to provide the best possible platforms to maintain standards for data security. These are routinely audited by BSI. Supplementary to existing BSI certifications, Bistech is currently implementing additional GDPR (General Data Protection Regulation) obligations, in accordance with the recently published British Standard (BS 10012:2017), against which further third party certification will be pursued once available.

5.6.3 People who contact us via social media. The practice does not use social media?

5.6.4 People who email us. Any email sent to us, including any attachments, may be monitored and used by us for reasons of security and for monitoring compliance with office policy. Email monitoring or blocking software may also be used. Please be aware that you have a responsibility to ensure that any email you send to us is within the bounds of the law.

Emails are stored on the secure NHS.net server and locally on the practice server. Access to both the practice server and NHS net accounts are password protected and managed by the local Commissioning Support Unit.

5.6.5 People who make a complaint to us. When we receive a complaint from a person, we make up a file containing the details of the complaint. This normally contains the identity of the complainant and any other individuals involved in the complaint. We will only use the personal information we collect to process the complaint and to check on the level of service we provide. We do compile and publish statistics showing information like the number of complaints we receive, but not in a form which identifies anyone. We usually have to disclose the complainant's identity to whoever the complaint is about. This is inevitable where, for example, the accuracy of a person's record is in dispute. If a complainant doesn't want information identifying him or her to be disclosed, we will try to respect that. However, it may not be possible to handle a complaint on an anonymous basis.

We will keep personal information contained in complaint files in line with our retention policy. This means that information relating to a complaint will be retained for ten years from closure. It will be retained in a secure environment, either electronically on the practice / One Domain server or as a paper record, and access to it will be restricted according to the 'need to know' principle.

6. Job applicants. For applications received via the NHS Jobs website, NHS Jobs are the data controller. Their privacy notice is at https://www.jobs.nhs.uk/privacy.html. For applications made directly to the

practice, Stoke Gifford and Conygre Road Medical Centre is the data controller for the information you provide during the process unless otherwise stated. If you have any queries about the process or how we handle your information please contact us.

6.1 What will we do with the information you provide to us? All of the information you provide during the process will only be used for the purpose of progressing your application, or to fulfil legal or regulatory requirements if necessary.

We will not share any of the information you provide during the recruitment process with any third parties for marketing purposes or store any of your information outside of the European Economic Area. The information you provide will be held securely by us and/or our data processors whether the information is in electronic or physical format.

We will use the contact details you provide to us to contact you to progress your application. We will use the other information you provide to assess your suitability for the role you have applied for.

What information do we ask for, and why? We do not collect more information than we need to fulfil our stated purposes and will not retain it for longer than is necessary. The information we ask for is used to assess your suitability for employment. You don't have to provide what we ask for but it might affect your application if you don't. The paper records of applicants not selected for interview will be destroyed after the initial sift. The paper records of candidates that were interviewed will be kept for 6 months and then securely destroyed.

6.2 Application stage. If you use the NHS jobs online application system, this will be collected by a data processor on our behalf (please see below). We ask you for your personal details including name and contact details. We will also ask you about your previous experience, education, referees and for answers to questions relevant to the role you have applied for. Our recruitment team will have access to all of this information.

You will also be asked to provide equal opportunities information. This is not mandatory information – if you don't provide it, it will not affect your application. This information will not be made available to any staff outside of our recruitment team, including hiring managers, in a way which can identify you. Any information you do provide, will be used only to produce and monitor equal opportunities statistics.

6.3 Shortlisting. Our hiring managers shortlist applications for interview. They will not be provided with your name or contact details or with your equal opportunities information if you have provided it.

6.4 Assessments. We might ask you to participate in assessment days; complete tests or occupational personality profile questionnaires; and/or to attend an interview – or a combination of these. Information will be generated by you and by us. For example, you might complete a written test or we might take interview notes. This information is held by the Practice.

If you are unsuccessful following assessment for the position you have applied for, we may ask if you would like your details to be retained in our talent pool for a period of six months. If you say yes, we would proactively contact you should any further suitable vacancies arise.

Final recruitment decisions are made by hiring managers. All of the information gathered during the application process is taken into account. You are able to ask about decisions made about your application by speaking to the management team

6.5 Conditional offer. If we make a conditional offer of employment we will ask you for information so that we can carry out pre-employment checks. You must successfully complete pre-employment checks to progress to a final offer. We are required to confirm the identity of our staff, their right to work in the United Kingdom and seek assurance as to their trustworthiness, integrity and reliability.

You will therefore be required to provide:

- Proof of your identity – you will be asked to attend our office with original documents, we will take copies.
- Proof of your qualifications – you will be asked to attend our office with original documents, we will take copies.
- You will be asked to complete a criminal records declaration to declare any unspent convictions.
- We will contact your referees, using the details you provide in your application, directly to obtain references

If we make a final offer, we will also ask you for the following:

- Bank details – to process salary payments
- Emergency contact details – so we know who to contact in case you have an emergency at work
- Membership of the NHSE Pension scheme – so we can send you a questionnaire to determine whether you are eligible to re-join your previous scheme.
- P45 information and any information about student loans that would need to be included in payroll.

6.6 Applications through NHS jobs website. The privacy statement for the NHS jobs website can be found at https://www.jobs.nhs.uk/privacy.html

7. Current and former employees

7.1 Health Pay. If you accept a final offer from us, some of your personnel records will be held by Healthpay. They provide our payroll services. Their privacy statement at http://www.healthpay.co.uk/privacy-notice/

7.2 NHS Pensions. Likewise, your details will be provided to the NHS Pensions Authority. You will be auto-enrolled into the pension scheme and details provided to the NHS Pensions Authority will be your name, date of birth, National Insurance number and salary. Your bank details will not be passed to the NHS Pensions Authority at this time.

7.3 Peninsula HR Service. The practice may, from time to time, consult with an external Human Resources Service for HR advice and guidance. In such instances, personal data will be shared with them. The Peninsula Privacy notice is at www.peninsulagrouplimited.com/privacy-policy-clients/ .

8. Your rights. Under the Data Protection Act 1998, you have rights as an individual which you can exercise in relation to the information we hold about you. You can read more about these rights here – https://ico.org.uk/for-the-public/is-my-information-being-handled-correctly/

8.1 Complaints or queries. Stoke Gifford and Conygre Medical Centres try to meet the highest standards when collecting and using personal information. For this reason, we take any complaints we receive about this very seriously. We encourage people to bring it to our attention if they think that our collection or use of information is unfair, misleading or inappropriate. We would also welcome any suggestions for improving our procedures.

This privacy notice was drafted with brevity and clarity in mind. It does not provide exhaustive detail of all aspects of the practice's data collection and use of personal information. However, we are happy to provide any additional information or explanation needed. Any requests for this should be sent to the address below.

Stoke Gifford and Conygre Medical Centres

Ratcliffe Drive, Stoke Gifford, Bristol, BS32 8UE

If you want to make a complaint about the way we have processed your personal information, you can contact us in our capacity as the statutory body which oversees data protection law – www.ico.org.uk/concerns.

8.2 Access to personal information. The practice tries to be as open as it can be in terms of giving people access to their personal information. Individuals can find out if we hold any personal information by making a 'subject access request' under the Data Protection Act 1998. If we do hold information about you we will:

- give you a description of it;
- tell you why we are holding it;
- tell you who it could be disclosed to; and
- let you have a copy of the information in an intelligible form.

To make a request to the practice for any personal information we may hold you need to put the request in writing addressing it to our Information Governance Lead, or writing to the address provided below. We have 30 calendar days to respond to this request but can extend this to 90 days if the request is complex. The reason for this extension would be explained to you within the initial 30 days of the request.

The practice will make data available via the on-line access portal or in PDF format and this will be emailed securely to your choice of email address. Information that is likely to cause harm or distress or that relates to third parties will be redacted.

Where repeated requests are made, in subsequent responses we will only provide the data that has been added since the auctioning of the previous request. There will be an administration charge where requests for information are manifestly unfounded, excessive or repetitive.

If you agree, we will try to deal with your request informally, for example by providing you with the specific information you need over the telephone. If we do hold information about you, you can ask us to correct any mistakes by contacting the Business Manager.

8.3 Access to the medical records of children. Parents will be able to request access to their children's records up to the age of 13 years. From 13 to 16 requests will for access from parents and children will be assessed on a case by case basis. The expectation is that, in all cases, parental access will be denied without the explicit consent of the child once the child is 16 years old.

A child may make a Subject Access Request in relation to their own personal data as from the age of 13 they are normally considered competent enough to do so.

8.4 Access by those with parental responsibility. Those with parental responsibility for a child under 13 years may make an access request on their behalf but the information holder must consider whether it is in the best interests of the child to disclose information held. The Practice will be guided by the guidance at https://www.gov.uk/parental-rights-responsibilities/who-has-parental-responsibility in relation to access to a child's records by the father.

8.5 Access Requests for those who lack capacity to consent. In certain circumstances a person acting as an advocate can seek access to personal information in so far as it is necessary or relevant to their role. This includes:

- Persons appointed by the Court of Protection
- Persons holding a registered Power of Attorney for specified purposes
- Persons appointed as Independent Mental Health Advocates under the Mental Capacity Act 2005

8.6. Right to rectification. If your data is incorrect, you have a right for it to be rectified and we will complete this rectification without delay. However, this right does not extend to over-riding a clinical decision.

8.7 Right to erasure. The Practice is governed by legislation relating to the NHS and we are legally obliged to process your data in the public interest or in the exercise of official authority vested in us as the data controller. As a result, the right to erasure of your medical data does not apply.

9. Disclosure of personal information. In many circumstances we will not disclose personal data without consent. However when we investigate a complaint, for example, we will need to share personal information with the organisation concerned and with other relevant bodies. Further information is available in our Information Charter about the factors we shall consider when deciding whether information should be disclosed.

10. Retention Periods. Data is retained in accordance with the NHS guidelines. For the GP records, data is maintained for 10 years after a patient's death. For staff records, it is maintained until the colleague is 75 or until 6 years after they left the practice.

11. Further information

You can also get further information on:

- agreements we have with other organisations for sharing information;
- circumstances where we can pass on personal data without consent for example, to prevent and detect crime and to produce anonymised statistics;
- our instructions to staff on how to collect, use and delete personal data; and
- how we check that the information we hold is accurate and up to date.

12. Links to other websites. This privacy notice does not cover the links within this site linking to other websites. We encourage you to read the privacy statements on the other websites you visit.

13. Changes to this privacy notice. We keep our privacy notice under regular review. This privacy notice was last updated on 30 May 2018.

14. How to contact us. If you want to request information about our privacy policy you can email us or write to Gavin Richards, Stoke Gifford Medical Centre, Ratcliffe Drive, Stoke Gifford, Bristol, BS34 8UE or gavin.richards@nhs.net)

Vers 5 Jul 19

Review –

Annexes

A. Caldicott Principles

Annex A

The Caldicott Principles (revised 2013)

Principle 1 - Justify the purpose(s) for using confidential information

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.

Principle 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).

Principle 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.

Principle 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.

Principle 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.

Principle 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.

Principle 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 .

Source: https://www.igt.hscic.gov.uk/Caldicott2Principles.aspx