Patient Privacy Information

Introduction

Healthcare professionals who provide you with care are required by law to maintain records about your health and any treatment or care that you have received. These records help us to provide you with the best possible medical care. Healthcare Group acts as 'controller' and determines the purposes and means of the processing of this personal data and complies with the Data Protection (Bailiwick of Guernsey) Law 2017. This document explains why the Healthcare Group collects information about patients and how we keep it safe and confidential, and how that information may be used.

Why we collect information about patients

Healthcare professionals need to maintain records about a patient's health and any treatment or care that they have received. We collect and hold data for the purpose of providing the best possible healthcare services to our patients. In carrying out this role we may collect information about patients, which helps us respond to their queries and medical concerns or secure for them specialist services. We may keep information about patients in a written or digital form. The records are retained in line with the Healthcare Policy on the Management and Retention of Records. As a basic principle electronic records would be kept indefinitely. Ten years after a patient has died or left the Practice, paper records may be confidentially destroyed.

Details we collect about patients

The records we collect include basic details, such as a patient's name and address. They will usually also include more sensitive information, known as 'special category data', about an individual's health and treatments they have received in the past.

Records that we hold may include:

- Details such as the patient's full name, patient ID number, title, gender, date of birth, address, next of kin, emergency contacts, telephone number, mobile phone number and email address.
- For the purposes of billing, a social security number, insurance provider and membership number and if you are supported by the States of Guernsey, we may hold a claim number for this.
- Any contacts with the surgery, such as appointments, clinic visits, immunisations, emergency appointments etc.
- Notes and reports about individual's health, treatment and care.
- Results of investigations, such as laboratory tests, x-rays etc.
- Relevant information from other health professionals, relatives or those who care for the individual.

How we use information about patients

We adhere to a strict code of confidentially regarding the management of patient information. Confidential patient data may be shared within the health care teams at the practices to ensure that patients can receive the services and care that they require. This includes the doctors, nurses, osteopaths, physiotherapists, secretaries and receptionists. Our staff only access information that is required to fulfil their roles and have a professional and contractual duty of confidentiality.

In some situations, a patient's health needs may require direct care from other healthcare providers or healthcare services outside of this Practice. In these situations, we will exchange with them information about you that is necessary for them to provide that care. Anyone with whom we share this information will have a professional and contractual duty of confidentiality.

Situations where your information may be shared for direct care include:

- Referral to a specialist or for specialist services.
- Referral for investigations such as x-rays, blood tests and other diagnostic investigations.
- With pharmacists for distribution of medications and other associated items.
- Community service providers when social care is required.
- Health and Social Care for inclusion into health screening programmes such as the bowel and breast cancer screening.
- Public Health for the notification of certain diseases such as food poisonings.

We only share information with others involved in your direct care when they have a genuine need for it. In all cases only the minimum amount of information to serve the purpose required would be released.

In order to function as a business and for the management of our medical services it is necessary for the Healthcare Group to hold and process some of your information for the purposes of billing.

Some of this information may be shared with the Office for Employment and Social Security in order to claim a grant contribution towards your consultation if you are eligible to receive this payment.

The legal basis for the Healthcare Group to process patient data

For the provision of direct patient care, consent for the Healthcare Group to process patient's data within and outside of the practice is assumed and is allowed under the Data Protection (Bailiwick of Guernsey) Law 2017 articles Schedule 2 Part II (10)

(a) The processing is necessary for a health or social care purpose….

(b) In subparagraph (a) –

'Health or social care purpose' includes the purpose of –

(i) Preventative or occupational medicine
(ii) The assessment of the working capacity of an employee or worker
(iii) Medical diagnosis
(iv) The provision of medical, health or social care or treatment, or
(v) The management of medical, health or social care systems and services

We will not share patient information with any third parties for reasons that are not for direct patient care unless you give us the explicit consent to do so, such as providing information to:

- Your employer
- Insurance companies
- Solicitors

Data may also be used for 'legitimate interests of our business' or 'for the conclusion or performance of a contract'. For example, to see that the Practice runs efficiently, plans for future services, trains its staff and receives monies due. Information may also be needed to help educate tomorrow's clinical staff and to carry out medical and other health research for the benefit of everyone.

In all other situations we would not disclose personal information about a patient without their consent unless there were exceptional circumstances (i.e. a life and death situation) or where disclosure is in the public interest or when there is a legal duty to do so, for example a court order. However, some anonymised data may be used at a local level to help plan for services.

Data Processors

Healthcare Group uses data processors to perform certain administrative tasks for us. These include:

(1) Next Generation IT (NGIT) – the Healthcare Group has a twenty-four hour / day contract with a local specialist IT company, NGIT. This includes a completely hosted solution which is designed to ensure complete security and no loss of continuity to our information technology network. The solution which encompasses SaaS (software as a service) IaaS (infrastructure as a service) are all housed within an accredited Data Centre with is certified ISO / IEC 27001:2013.

(2) Microtest Evolution – this hosts the electronic GP patient records database. All information is hosted in an accredited data centre managed by NGIT.

(3) Medibooks – this generates the billing information relating to services provided to the Healthcare Group patients. No individual's banking details are stored on this platform. This is housed within an accredited data centre managed by NGIT.

(4) Roman Cart – this provides an online payment facility for patients on the Healthcare website

(5) Microsoft Outlook – the Healthcare Group emailing system. This is encrypted and may be used to transfer patient information to other secure email addresses. This is housed in an accredited data centre managed by NGIT.

(6) Sunquest ICE – this enables the pathology system based at the Princess Elizabeth Hospital to send pathology information to the Microtest Evolution server, so that pathology results can be accessed by healthcare professionals within Healthcare Group. This is housed in an accredited data centre managed by NGIT.

(7) Archivist – Secure storage facility for the retention of patient paper notes. This is managed in line with our Management and Retention of Records Policy.

We ensure that the data processors that support us are legally and contractually bound to operate and prove security arrangements are in place, and our fully compliant with the data protection law.

Healthcare Group's Data Protection Officers

Under the Data Protection Law, Healthcare Group is required to have a Data Protection Officer(s). Their role is:

(1) To inform and advise the organisation and its employees about their obligations to comply with DPL the data protection laws
(2) To monitor compliance with the Data Protection Laws, including managing internal data protection activities, advise on data protection impact assessments; train staff and conduct internal audits
(3) To be the first point of contact for supervisory authorities and for individuals whose data is processed.

At the Healthcare Group, our Data Protection Officer is:

- The Central Services Manager

Patient rights under the Data Protection (Bailiwick of Guernsey) Law 2017

The right of access, rectification and erasure

Patients have the right to access their personal data. It is the Healthcare Group's policy that access requests should be put in writing to the Data Protection Officer. However, if this is not possible a verbal request can be made. Upon receipt of a request, the records will be reviewed by a doctor to ensure that there is no reason why the records should not be released. We would aim to provide the information within one month, however, this may be extended by a further two months if the request is complex.

As a general rule there is no charge for providing this information as long as the request is reasonable. However, an administrative fee may be charged for repetitive or unfounded requests. Requests from insurance companies and employers are not regarded as subject access requests and will be subject to a charge.

Although in most cases, patients have the right to access information held about them, there may be some circumstances when a GP believes that giving a patient access to the information held about them, may cause serious harm to the physical or mental health or condition of the individual or another person, or identify another person. This may justify refusing disclosure for all or part of the records.

If a patient or carer wishes to correct any inaccurate information, they believed is held about them, they should initially contact the Data Protection Officer in writing detailing their concerns. We would aim to respond to the concern within one month, although this can be extended by two months where the request is complex. It may be the case that we cannot delete the relevant record or entry, because it is important that the entry, assessment and explanation or medical opinion be retained so that there is an understanding and explanation of subsequent events (such as how a patient was treated, or what further tests were organised) in their medical history.

Where we are not able to delete information, we can add a note to the disputed entry explaining your remaining concerns and we can offer the patient the option of adding an addendum of their own.

Please be aware that an alteration to an electronic record, or deletion of an entry in it, is always preserved (together with the original entry) as part of the electronic audit trail.

If a patient remains dissatisfied with the outcome of their request they can make an official complaint to the Healthcare Group or contact the Office of the Data Protection Authority Tel No: (01481 742074) or email: enquiries@odpa.gg

The right to object and to restrict processing

We would always try and respect the wishes of a patient if they did not want their data to be used in a particular way, unless to do so would mean that we could not provide you with safe and effective medical care.

Patients have the right to object to primary uses of your medical record; that is the sharing of their data with health professionals outside of the surgery for the provision of direct medical care, if you so wish.

Patients also have the right to object to secondary uses of your medical records; that is the sharing of their data for purposes unrelated to your direct medical care, such as anonymised data which is used at a local level to help the States of Guernsey plan services.

If a patient wishes to object to how their data is being processed, they should ideally discuss this with their doctor first and then contact the Data Protection officer if they wish to take this further.

The right to data portability

This right only applies to information a patient has given us. In this situation the patient has the right to ask that we transfer the information they have given us from one organisation to another or arrange for them to be given a copy. The right only applies if we are processing information based on consent or under a contract (or in conjunction with a potential contract) and the processing is automated.

The right to withdraw consent

Patients have the right to withdraw their agreement for us to hold information we retain on the legal basis of requiring consent at any time. This may include the release of information to certain parties such as a family member or receiving information via emails for example.

The right not to be subject to decisions based on automated processing

Patients have the right not be subject to a decision based solely on automated means.

Retention of data

We retain data for no longer than necessary for the purposes we have set out above. As a principle electronic health records are kept indefinitely but would be deducted and restrictions to access applied if a patient was to leave our practice. Paper records are confidentially destroyed 10 years after a patient dies or leaves the practice. Information we hold for the purposes of billing is usually deleted after 6 years. Further information on the Healthcare Groups policy on the management, retention and destruction of records can be provided if required.

The use of emails

We fully understand that our patients like to use emails as a means of communication.

At Healthcare Group we have a secure email system with the ability to send encrypted emails to certain recipients. However, we cannot guarantee the secure transmission of emails to personal email accounts.

Data Breaches

A personal data breach means a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

If we become aware of a breach in confidentiality that is likely to result in a risk to the rights and freedoms of individuals, we are obliged to inform the Office of the Data Protection Authority within 72 hours The report must give a description of the breach and how it happened. It must also include the list of the personal details breached and the likely consequences following the breach. Action plans to prevent further breaches will need to be submitted. Likewise, we must inform the individuals concerned without undue delay.

If a patient has a concern that a breach of their personal data has taken place, they should contact the Data Protection Officer immediately, so that this can be fully investigated.

How to Complain

If you have a complaint regarding your data or privacy, you can either complain to Healthcare's Data Protection Officer or to the Office of the Data Protection Authority on 742074 or email: enquiries@odpa.gg