General Data Protection Policy

Introduction

Renal Services (UK) Ltd is required to collect and maintain certain personal data about individuals (patients, employees, clients, suppliers and job applicants) for the purposes of satisfying operational obligations. The company recognises the importance of correct and lawful treatment of personal data; it maintains confidence in the organisation and provides successful operations.

The type of personal data that may be required includes information about: current, past and prospective employees and patients; suppliers and others with whom the company communicates. The personal data, whether it is held on paper, on computer or other media, will be subject to the appropriate legal safeguards as specified in the Data Protection Act 1998.

To this end Renal Services (UK) Ltd fully endorses and adheres to the eight principles of the Data Protection Act. These principles specify the legal conditions that must be satisfied in relation to obtaining, handling, processing, transportation and storage of personal data. Employees and any others who obtain, handle, process, transport and store personal data for the company must adhere to these principles.

Renal Services (UK) Ltd is registered with the Information Commissioner's Office (ICO), who is responsible for the promotion and enforcement of the Data Protection Act 1998.

1. Data Protection Act 1998

1.1. Principles

The eight principles require that personal data shall:

1.1.1. Be processed fairly and lawfully and shall not be processed unless certain conditions are met;
1.1.2. Be obtained for a specified and lawful purpose and shall not be processed in any manner incompatible with that purpose;
1.1.3. Be adequate, relevant and not excessive for those purposes;
1.1.4. Be accurate and, where necessary, kept up to date;
1.1.5. Not be kept for longer than is necessary, kept up to date;
1.1.6. Be processed in accordance with the data subject's rights;
1.1.7. Be kept secure from unauthorised or unlawful processing and protected against accidental loss, destruction or damage by using the appropriate technical and organisational measures;
1.1.8. Not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of protection for the rights and freedom of data subjects in relation to the processing of personal data.

1.2. Satisfaction of Data Protection Principles

In order to meet the requirements of the principles, Renal Services (UK) Ltd will:

1.2.1. Observe fully conditions regarding the fair collection and use of personal data;

1.2.2. Meet its obligations to specify the purposes for which the information is used;
1.2.3. Collect and process appropriate personal data only to the extent that it is needed to fulfil operational or any legal requirements;
1.2.4. Ensure the quality of personal data used;
1.2.5. Apply strict checks to determine the length of time information is held;
1.2.6. Ensure that the rights of individuals about whom the personal data is held can be fully exercised under the Act. (These include: The right to be informed that processing is being undertaken, the right of access to one's personal information, the right to prevent processing in certain circumstances and the right to correct, rectify, block or erase information which is regarded as wrong information);
1.2.7. Take the appropriate technical and organisational security measures to safeguard personal date;
1.2.8. Ensure that personal data is not transferred abroad without suitable safeguards.

2. Policy Scope

2.1. This policy applies to:

2.1.1. The Head Office and all dialysis units of Renal Services (UK) Ltd
2.1.2. All staff and volunteers of Renal Services (UK) Ltd
2.1.3. All contractors, suppliers and other people working on behalf of Renal Services (UK) Ltd

2.2. It applies to all data that the Company holds relating to identifiable individuals, even if that information technically falls outside of the Data Protection Act 1998. This can include:

2.2.1. Names of individuals
2.2.2. Postal addresses
2.2.3. Email addresses
2.2.4. Telephone numbers
2.2.5. Health records plus any other information relating to individuals

3. Responsibility

3.1. Everyone who works for or with Renal Services (UK) Ltd has some responsibility for ensuring data is collected, stored and handled appropriately.

3.2. Each team that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

However, the following people have key areas of responsibility:

3.3. The board of directors is ultimately responsible for ensuring that Renal Services (UK) Ltd meets its legal obligations.

3.4. The data protection officer, Glen Ewing is responsible for:

3.4.1. Keeping the Board of Directors updated about data protection responsibilities, risks and issues.

3.4.2. Reviewing all data protection procedures and related policies, in line with an agreed schedule.
3.4.3. Arranging data protection training and advice for the people covered by this policy.
3.4.4. Handling data protection questions from staff and anyone else covered by this policy
3.4.5. Dealing with requests from individuals to see the data Renal Services (UK) Ltd holds about them (also called 'subject access requests').
3.4.6. Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data.
3.4.7. Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
3.4.8. Performing regular checks and scans to ensure security hardware and software is functioning properly.
3.4.9. Evaluating any third-party services the company is considering using to store or process data. For instance, cloud computing services.

3.5. The Marketing Data Protection Compliance Officer, Marta Lago, is responsible for:

3.5.1. Managing and ensuring compliance of the marketing communications data base
3.5.2. Approving any data protection statements attached to communications such as emails and letters.
3.5.3. Addressing any data protection queries from journalists or media outlets.
3.5.4. Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles.

3.6. The Operations Data Protection Officer, Neluka Weerasooriya, is responsible for:

3.6.1. Managing any data and communications in relation to the operational delivery of client services.
3.6.2. Managing any data and communications with renal services patients or patients wishing to attend our clinics for holiday dialysis.

3.7. The Finance Data Protection Officer, Isaac Dossa, is responsible for:

3.7.1. Managing any data and communications in relation to suppliers, contractors or clients.

3.8. The HR Data Protection Officer, Kamini Kotak, is responsible for:
3.8.1. Managing any data and communications in relations to members of staff employed or previously employed by Renal Services
3.8.2. Managing any data in relation to job applicants

4. General Staff Guidelines

4.1. Access to personal data covered by this policy will only be given to those who require it for their work;

4.2. Data should not be shared informally. When access to confidential information is required, employees can request it from their line managers, who will then get the approval of the data release from the relevant data protection compliance officer;

4.3. Renal Services (UK) Ltd will provide training to all employees to help them understand their responsibilities when handling data;

4.4. Employees should keep all data secure, by taking sensible precautions and following the guidelines below;

4.5. In particular, strong passwords must be used and they should never be shared.

4.6. Personal data should not be disclosed to unauthorised people, either within the company or externally;

4.7. Data should be regularly reviewed and updated if it is found to be out of date. If no longer required, it should be deleted and disposed of;

4.8. Employees should request help from their line manager or the data protection compliance officer for their department, if they are unsure about any aspect of data protection.

5. Confidentiality

5.1. All information recorded in patient notes or on the computer system is confidential and should not be released to unauthorised members of staff, patients, patient's relatives or friends, without following appropriate procedures or without the patient's consent;

5.2. Patient information is generally held under legal and ethical obligations of confidentiality. Therefore, information provided in confidence should not be used or disclosed in a form that might identify a patient without his or her consent;

5.3. Patients entrust the clinical staff with sensitive information relating to their health and other matters as part of their treatment;

5.4. The organisation understands that a duty of confidence arises when one discloses information to another in circumstances where it is reasonable to expect that the information will be held in confidence. It therefore is;

5.5. A legal obligation that is derived from case law;

5.6. A requirement established with professional codes of conduct;

5.7. A part of the employment contract within the organisation linked to disciplinary procedures for the unlawful disclosure of personal information;

5.8. The organisation will follow the guidelines on the use and protection of patient information as laid out in The NHS Confidentiality Code of Practice November 2003.

6. Data Storage

6.1. All data storage queries need to be directed to the relevant data protection compliance officer

6.2. When data is stored on paper, it should be kept in a secure place where unauthorised people cannot see it.

6.3. When not required, the paper or files should be kept in a locked drawer or filing cabinet;

6.4. Employees should make sure paper and printouts are not left where unauthorised people could see them, like on a printer;

6.5. Data printouts should be shredded and disposed of securely when no longer required.

6.6. When data is stored electronically, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:

6.6.1. Data should be protected by strong passwords that are changed regularly and never shared between employees;
6.6.2. If data is stored on removable media, these should be kept locked away securely when not being used.
6.6.3. Data should only be stored on designated drives and servers, and should only be uploaded to an approved cloud computing service;
6.6.4. Data should be backed up frequently. Those backups should be tested regularly, in line with company's standard backup procedures;
6.6.5. All servers and computers containing data should be protected by approved security software and a firewall.

7. Health Records

7.1. A health record is defined within the Data Protection Act 1998 as a record consisting of information about the physical or mental health or condition of an identifiable individual made by or on behalf of a health professional in connection with the care of that individual;

7.2. The Data Protection Act 1998 governs access to health records of living people and became effective from 01 March 2000. It superseded the Data Protection Act 1984 and Access to Health Records Act 1990 with the exception of the deceased persons. The Access to Health Records Act 1990 still governs the access to the health records of deceased people;

7.3. The Data Protection Act 1998 gives every living person in the UK or their authorised representative the right to apply for access to their health records irrespective of when they were complied. It also gives access to patients who now reside outside the UK the right to apply for access to their former UK health records;

7.4. Applications to access health records received by Renal Services will follow guidelines laid out by the Department of Health – Guidance for Access to Health Records Requests under the Data Protection Act 1998;

7.5. All applications to access health records for contracted NHS patients will be forwarded to the referring NHS Trust.

8. Data Use

8.1. Personal data is of no value to Renal Services (UK) Ltd unless the business can make use of it. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption and theft.

8.2. When working with personal data, employees should ensure the screens of their computers are always locked when left unattended.

8.3. Personal data should not be shared informally. In particular, it should never be sent by email, as this form of communication is not secure.

8.4. Data must be encrypted before being transferred electronically. The compliance officer can explain how to send data to authorised external contacts.

8.5. Personal data should never be transferred outside the European Economic Area.

8.6. Employees should not save copies of personal data on their own computers. Always access and update the central copy of any data.

9. Guidelines for safe and secure data sharing

9.1. It is sometimes necessary to share confidential information The Company will ensure data sharing is in line with the following:

9.2. **Sharing personal information by phone**

9.2.1. Identify the person requesting information by confirm the name, job title, department and organisation;
9.2.2. Ensure the reason for request of the information is appropriate
9.2.3. Take a contact telephone number;
9.2.4. Check if information can be provided. If in doubt inform enquirer that you need to clarify with a manager/ senior personnel prior to giving out the information and call them back later;
9.2.5. Provide information only to the enquirer (do not leave messages);
9.2.6. Make record of request for information and information disclosed along with the recipient's name, job title, organisation, telephone number. Sign and date record.

9.3. **Sharing personal information by fax**

If the information is being faxed to a known safe haven/secure fax it is not necessary, follow any special instructions. If not;

9.3.1. Telephone the recipient of the fax to confirm the transmission prior to sending confidential information;
9.3.2. Re-check fax number prior to sending the information;
9.3.3. Ensure the receipt of the fax is acknowledged;
9.3.4. Use fax cover sheet at all times. Ensure the recipient's name is legible and mark it 'private and confidential';
9.3.5. If appropriate, request a report sheet to confirm that transmission;
9.3.6. File the report in the appropriate patient notes;

9.4. **Sharing personal information by post**

9.4.1. Confirm name, department and address of recipient;
9.4.2. Seal the information in a robust envelope;
9.4.3. Mark the envelope 'private and confidential – to be opened by addressee only';
9.4.4. Send by recorded delivery when appropriate;
9.4.5. Request confirmation of receipt;

10. Data Accuracy

10.1. The law requires Renal Services (UK) Ltd to take responsible steps to ensure data is kept accurate and up to date.

10.2. The more important it is that the personal data is accurate, the greater the effort Renal Services (UK) Ltd should put into ensuring its accuracy.

10.3. It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

10.4. Data will be held in as few places as necessary. Staff should not create any unnecessary additional data sets.

10.5. Staff should take every opportunity to ensure data is updated. For instance, by confirming customers details when they call.

10.6. Data should be updated as inaccuracies are discovered. For instance, if a customer can no longer be reached on their stored telephone number, it should be removed from the database.

10.7. It is the Chief Development Officer's responsibility to ensure marketing databases are checked against industry suppression files every six months.

11. Retention and Storage of patient records

11.1. All holiday/transient patients attending treatment will have their dialysis specific records kept within the department until their eventual discharge/transfer from the service. Once they have been discharged/transferred the records will be forwarded to the head office for archiving;

11.2. All contract patients from the local NHS trust will have their dialysis specific records kept within the department until their eventual discharge/transfer from the service. Once they have been discharged/transferred the relevant records will be sent back to the NHS trust for archiving;

11.3. All records with the recent six-month period for patient from the local NHS trust will be kept in the dialysis unit file. Excess records will be forwarded to the NHS trust for archiving;

11.4. All service users will have their records kept in designated dialysis folders, which will be retained on the Unit until their discharge/transfer;

11.5. When not in use records will be kept in the designated locked drawers in the dialysis unit. The Unit is secured out of hours;

11.6. All records of holiday/transient patients will be sent to head office for archiving within one week of the patient's discharge/transfer from the service;

11.7. All information received for holiday/transient patients from outside sources will be shredded once no longer needed;

11.8. Medical record sheets for the dialysis unit constitute;

11.8.1. Dialysis flow charts
11.8.2. Outpatient prescription charts
11.8.3. Nursing evaluation, communication and care planning
11.8.4. Clinical information
11.8.5. Nursing admission profile
11.8.6. All patient treatments are to be logged in the statistics and machine folders for tracking and audit purpose.

12. Subject Access Request

12.1. All individuals who are the subject of personal data held by Renal Services (UK) Ltd are entitled to:

12.1.1. Ask what information the company holds about them and why.
12.1.2. Ask how to gain access to it.
12.1.3. Be informed how to keep it up to date.
12.1.4. Be informed how the company is meeting its data protection obligations.

12.2. If individuals contacts the company requesting this information, this is called a subject access request.

12.3. Subject access requests from individuals should be made by email, addressed to the data controller at (e-mail address).

12.4. Individuals will not be charged for a subject access request. The data controller will aim to provide the relevant data within 14 days.

12.5. The data controller will always verify the identity of anyone making a subject access request before handing over any information.

13. Disclosing data for other reasons

13.1. In certain circumstances, the Data Protection Act allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

13.2. Under these circumstances, Renal Services (UK) Ltd will disclose requested data. However, the data controller will ensure the request is legitimate, seeking assistance from the board and from the company's legal advisers where necessary.

14. Providing Information

14.1. Renal Services (UK) Ltd aims to ensure that individuals are aware that their data is being processed, and that they understand:

14.1.1. How the data is being used
14.1.2. How to exercise their rights

14.2. To these ends, the company has a privacy statement, setting out how data relating to individuals is used by the company.

14.3. This is available on request. A version of this statement is also available on the company's website.

References:

European Commission, General Data Protection Regulations April 2016
Data Protection Act 1998
Confidentiality – NHS Code of Practice; Department of Health; November 2003
Guidance for Access to Health Records Request under the Data Protection Act 1998; June 2003
Making a Difference: Safe and Secure Data Sharing Between Health and Adult Social Care Staff; Department of Health