CITY HEALTH CLINIC | 9 EARL GREY STREET | EDINBURGH | EH3 9BN

Data Protection, Confidentiality and Information Security Policy

Policy Statement

The company processes personal data that relate to employees and patients and is therefore required by law to comply with the General Data Protection Regulation, EU 2016 (GDPR), which protects the privacy of individual personal data and ensures that they are processed fairly and lawfully. The Practice is committed to ensuring that it complies with the GDPR and applies ethical principles to all aspects of its work to protect the interests of employees and patients and maintain the confidentiality and security of any personal data held in any form by the practice. To do this, City Health Clinic will comply with the eight principles in the General Data Protection Regulation. In summary, these state that personal data shall be:

1. fairly and lawfully processed;
2. processed for limited purposes (i.e. obtained only for specified and lawful purposes and further processed only in a compatible manner);
3. adequate, relevant and not excessive;
4. accurate and up to date;
5. not kept for longer than is necessary;
6. processed in line with the individual's rights.
7. Ensures appropriate security of personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical knowledge or organisational measures.
8. not transferred to countries outside the European Economic area without adequate protection.

Responsibilities

This Data Protection, Confidentiality and Information Security Policy applies to all practice employees and others who have legitimate rights to access and use the practice's information systems.

Compliance with GDPR and this policy is the responsibility of all practice employees and everyone who has access to practice records. A breach of this policy, whether deliberate or through negligence, could lead to disciplinary action being taken and possible investigation by the General Dental/Medical Council. A breach of GDPR could also lead to criminal prosecution.

The following table lists key responsibilities among the dental and medical team.

Dental Team Member	Responsibility
Yvonne Louden (Practice Manager)	General Data Protection Regulation, Confidentiality and Information Security policy; deals with subject access requests made under GDPR and requests made under the Freedom of Information Act (Scotland) 2002; training of staff regarding data protection and confidentiality.
Yvonne Louden	Appointed company Data Protection Officer
City Health Clinic Limited	Data controller (i.e. principal dentist who 'owns' a patient list)
Stephanie Laing	Data controller (i.e. principal dentist who 'owns' a patient list)
Ciara Sutherland	Data controller (i.e. associate dentist who 'owns' a patient list)
Irene Cullinane	Data controller (i.e. associate dentist who 'owns' a patient list)
Jemma Whyte	Data controller (i.e. associate dentist who 'owns' a patient list)
Bebhinn O'Neill	Data controller (i.e., VT under the umbrella of VT Trainer- Dr S Laing)
Dr Allison Thomas	Data controller (i.e. doctor who 'owns' a patient list)
Dr Jason Twinn	Data controller (i.e. doctor who 'owns' a patient list)
Dr David Richardson	Data controller (i.e. doctor who 'owns' a patient list)
Dr Shona Williamson	Data controller (i.e. doctor who 'owns' a patient list)
All staff	Compliance with the GDPR and this Data Protection, Confidentiality and Information Security policy

**If you have any questions or comments about processing personal data or this policy, please contact the Practice Manager.

Definition of Personal Data Covered Under GDPR

GDPR covers all personal data, regardless of the format, that are stored in a 'relevant filing system'. A relevant filing system means any system where information can be found relatively easily, even if it is not by a personalised index or key. In addition, information recorded with the intention that it will be put in a relevant filing system or held on computer is covered.

As an employer and to provide effective care for patients and provide care within the NHS system, the Practice processes personal data of employees and patients. Personal data means practically any information about, or correspondence relating to, a named individual. It includes both facts (e.g. treatment a patient has had) and opinions (e.g. any concerns the patient or dental / medical team might have about the patient's dental or medical health), including:

a) personal information and contact details, including the patient's name, address and date of birth;
b) dental, social and medical histories (e.g. past or current medical conditions, current medication, the name of the patient's GP, special needs);
c) results of the examination of the patient's mouth and oral health, including x-rays and clinical photographs;
d) personal information relating to patient Health Screen reports, GP records and Occupational Health Assessment reports
e) information about appointments;
f) any treatments and their costs;
g) any proposed care, including advice given to the patient and referrals the patient might need;
h) any concerns that the patient or dental or medical team might have;
i) details of the patient's consent for specific procedures;
j) correspondence with other healthcare workers that relates to the patient's care.

Procedures for Ensuring Compliance with GDPR and the Confidentiality and Security of Personal Data

All Staff

To maintain a good patient dental / medical team relationship, it is essential that patients feel they can provide personal information to dental and medical team members with the knowledge that this information will be kept securely and not shared unlawfully. It is also important that patients are able to provide, in confidence, full details of their medical, social and dental histories to facilitate safe and effective care. To achieve this, all staff must follow the procedures listed below.

- Comply with the principles outlined in the General Dental Council principles set out in the '*Standards for Dental Professionals guidance*', and the General Medical Council for '*Good Medical Practice*' and the Dental Standards in '*Principles of Patient Confidentiality* 'and '*Principles of Patient Consent*'.
- Undergo training in processing personal data and confidentiality.
- Keep any personal data or confidential data that they hold, whether in electronic or paper format, securely, which includes:
  - storing paper files with personal data in filing cabinets that are locked when authorised staff are not present to monitor access;
  - storing electronic files containing personal data on password-protected computer systems;
  - 'screen-locking' unattended computers;

- not sharing computer passwords with unauthorised people, not writing down passwords and not keeping passwords on or near their computer;
- not forwarding emails containing personal data to internet email accounts as these are not secure;
- holding personal data on laptops only where there is a clear business necessity and permission is sought from the Practice Manager (if there is a necessity, ensure it is fully encrypted. * Note we do not at this time have business laptops for business use);
- avoiding carrying personal data on removable media (e.g. memory sticks or CD-roms);
- not using unlicensed software on Practice computers;
- ensuring windows and doors are secured if you are the last to leave the practice.
- Do not contact patients for marketing purposes without patient consent being obtained in the form of either signed patient consent, or by direct patient email consent.

➢ Practice good record-keeping, and ensure records are:

- accurate;
- dated;
- contemporaneous;
- comprehensive;
- secure;
- legible and written in language that can be read and understood by others, and is not derogatory.

➢ Maintain the confidentiality of any personal data by, for example:

- ensuring that personal information is not disclosed either orally or in writing, accidentally or otherwise, to any unauthorised third party (e.g. avoid working on personal data such as application forms on public transport, do not discuss identifiable information about patients with anyone outside the practice, including friends, family and schools, or leave messages about a patient's care with an unauthorised third party or on an answering machine) (NB: this also applies after termination of employment);
- respecting patient privacy for discussions of a sensitive nature (e.g. discussion of medical information, payment, or asking patients for proof of exemption status);
- using personal data only for the purposes for which they are authorised in the relevant Data Protection registration.
- Upholding a patient's request to erase or amend any information held on their record that that is proven to be inaccurate or incorrect.

- Ensure patients know what information is to be shared, why it is being shared and the likely consequences of sharing (or not sharing) the information and give patients the opportunity to withhold permission to share their information.
- Share personal data only on a 'need to know' basis and after signed consent is in place from the patient; for example:
  - to another health professional for the provision of effective care and/or treatment,
  - to ensure the provision of care under the NHS (e.g. payment claims, information for health boards, GP17).
  - to a third-party referrer i.e., private health service companies requesting occupational health reports etc., where our doctors have undertaken work on their direct instruction and where report results are issued with patient consent to the referrer.
  - Corporate clients referring employees for health screens will be invoiced showing patient attendance history and the billed service fee only. Personal information relating to the health screen is private, confidential and will not be disclosed to the employer. Consent to share this information is held on the patient's 'medical history questionnaire'.

- Check that any personal information that you provide in connection with your employment is accurate and up to date and inform the Practice Manager of any changes to this information.
- Inform the Practice Manager, who is responsible for ensuring compliance with GDPR and this policy, of any suspected or actual breach of the GDPR or this policy.

Clinicians

Clinicians must follow the procedures detailed above for staff, and the procedures listed below.

- Register with the UK Information Commissioner.
- Keep the details of the registration up to date and renew this registration annually.

General Practices

All staff contracts and agreements include a clause regarding the confidentiality and security of personal data.

- Keys for lockable storage cabinets are held only by dental and medical team members who require regular access to the information they contain. Keys are stored in a secure key cabinet.
- Practice computers have a full audit trail facility to prevent deletion or overwriting of data.
- Each computer is fitted with anti-virus and firewall software.
- Daily back-ups of the Practice's electronic records are made by our IT provider (ITCentric) and Patient Management System provider (Software of Excellence).
- Back-ups are tested by our IT provider (ITCentric) to ensure data can be retrieved in a useable format.
- Old PC's are removed from our premises and safely decommissioned by our IT provider ITCentric in accordance with data protection regulations, the hard drive is sanitized, removed and destroyed so the information contained cannot be accessed.
- Adult dental patient records are kept for at least 11 years; child patient records are kept for at least 11 years or until the patient is 25 years old, whichever is longer.
- Adult medical records are held as follows:

  Adults - Health Screens 10 years or 3 years after patient death, GP Records – Lifetime or 10 years after a patient death or after they have left the UK unless they remain in the EU.
- Personal data are reviewed, updated and deleted in a confidential and secure manner when no longer required.
- The clinic is based at Princes Exchange, there are security guards based on site 24 hours a day, including weekends and public holidays who monitor CCTV cameras placed around this building, they do a walk around to inspect the premises and act in accordance with their job role should there be any incident regarding a potential break-in or accident.

Sharing Personal Information

To provide the patient with appropriate care, we might need to share personal data with:

- another dentist or another health professional who is caring for the patient;
- the patient's GP;
- a dental or medical laboratory;
- NHS payment authorities;
- the Inland Revenue;
- the Benefits Agency, if the patient is claiming exemption or remission from NHS charges;

- a private dental scheme, if the patient is a member.
- In these cases, only the minimum information required will be shared.
- A medical patient's employer for appointment history and billing purposes with their consent
- Third party referrer (signed patient consent is in place prior to any medical being undertaken)

Disclosure Without Consent

Exceptional circumstances might override the duty to maintain confidentiality.
Where possible, we will inform the patient of requests to share personal information. The decision to disclose information must only be taken by senior staff. Examples include:

- situations where there is a serious public health risk or risk of harm to other individuals;
- when information is required by the police to prevent or detect crime or to apprehend or prosecute offenders (if not providing the information would prejudice these purposes);
- in response to a court order;
- to enable a dentist to pursue a legal claim against a patient.
- to enable a doctor to pursue and legal claim against a patient.

Dr Stephanie Laing, principal dentist, Dr Allison Thomas (senior doctor) and Yvonne Louden, practice manager are responsible for making the decision regarding whether personal data should be disclosed.

Subject Access Requests

Individuals have a right under the Data Protection regulation to have a copy of the information held about them on computer and in manual filing systems. This is known as the right of subject access. Parents also have rights to access their children's records if it is in the child's interest. The 'data controller' (i.e. the company, dentist or doctor) must make a judgement if a child or parent requests records (Data protection regulation allows a young person of 12 years or more in Scotland, with sufficient capacity and maturity, to exercise their rights under the Act). A solicitor can request access with the consent of his client.

A data protection policy that outlines the personal data that are processed and the manner in which the data are processed is available for patients.

The Practice Manager deals with subject access requests and will respond to requests from patients or employees within 30 days of receipt of the request. No fee will be levied unless a dental patient requests that a dental x-ray be sent to London for another identical x-ray to be produced, this is a specialised technique and the invoiced fee would be passed onto the patient. Dental x-rays can be photographed at no charge to the patient.

The following staff have read and understood this policy.

Dental Team Member	Position	Signature	Date
Dr Stephanie Laing	Principle Dentist		
Dr Ciara Sutherland	Dentist		
Dr Jemma Whyte	Dentist		
Dr Bebhinn O'Neill	Dentist		
Dr Mary Masterton	Dentist		
Dr William Donovan	Dentist		
Dr Allison Thomas	Lead Doctor		
Dr David Richardson	Doctor		
Dr Jason Twinn	Doctor		
Dr Shona Williamson	Doctor		
Yvonne Louden	Practice Manager		
Alexandra Graham	Assistant Manager		
Kirsty Wales	Medical Snr Administrator Receptionist		
Robyn Leitch	Acting Assistant Manager		
Bobby Beatson-Evans	Snr Dental nurse		
Kerry Kervin	Snr Dental nurse		
Samantha Carlisle	Receptionist Dental Nurse		
Carroll Leitch	Receptionist, Administrator		
Shellby Raynes	Receptionist Dental Nurse		
Kimberley Richardson	Receptionist Dental Nurse		

Yvonne Louden, practice manager Signature:

Policy last updated: 04/05/2018 Date of next review: May 2019