## GDPR Privacy Policy

This Policy document encompasses all aspects of security surrounding confidential client and company information. All company employees must read this document in its entirety and sign confirming they have read and fully understand this policy. This document will be reviewed and updated by Management on an annual basis or when relevant to include newly developed security standards into the policy and re-distributed to all employees and contractors where applicable.

1. CK Clinic ("The Company") handles sensitive cardholder information, personal identifiable information, personal medical records and notes pertaining to the assessment and treatment of all clients.
2. Sensitive Information must have adequate safeguards in place to protect the data, privacy, and to ensure compliance with various regulations and legislations.
3. The Company commits to respecting the privacy of all its clients and to protecting any sensitive information from outside parties. To this end management are committed to maintaining a secure environment in which to process and store personal information so that we can meet current legislation and professional standards of conduct. In addition The Company shall provide when requested any and all information held for a client without delay.

### Data types

The GDPR has defined data types into two headings;

- Personal data
- Specific Categories of Personal Data (Known as Sensitive personal Data under DPA)

The GDPR defines Personal Data as;

Any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mentalm, economic, cultural or social identity of that natural person.

The GDPR defines Special Categories of Personal Data as;

The processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning the health or data concerning a natural persons sex life or sexual orientation.

In this documents we will refer to these data types as "sensitive information".

### Caldicott

The term Caldicott refers to how patient information is processed and used with the public and private health sector and its sub contractors. There are seven Caldicott priciples;

**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.

In April 2013, Dame Fiona Caldicott reported on her second review of information governance, her report"Information: To Share Or Not To Share? The Information Governance Review", informally known as the Caldicott2 Review, introduced a new 7th Caldicott Principle.

**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

## Record Keeping

The records we keep in healthcare need to be clear, accurate, honest and timely. Accurate and up to date health and social care records;

- Are required under professional codes of conduct and contract of employmeny
- Facilitate clinical decision making
- Improve patient care
- Clearly communicate the treatment rationale
- Make sure we are accountable and reflects the quality of the care given
- Helps defend complaints or legal proceedings

## Employees handling sensitive data should ensure:

- Handle Company and Client information in a manner that fits with their sensitivity and classification;
- Limit personal use of the Company information and telecommunication systems and ensure it doesn’t interfere with your job performance;

- The Company reserves the right to monitor, access, review, audit, copy, store, or delete any electronic communications, equipment, systems and network traffic for any purpose;
- Do not disclose personnel information unless authorised;
- Protect sensitive information;
- Keep passwords and accounts secure;
- Do not install unauthorised software or hardware, including modems and wireless access unless you have explicit management approval;
- Always leave desks clear of sensitive data and lock computer screens when unattended;
- Information security incidents must be reported, without delay, to the individual responsible for incident response locally – Chris Kempson, Director CK Clinic

## Acceptable Use

Management is committed to protecting the clients, employees, partners and the Company from illegal or damaging actions, either knowingly or unknowingly by any individual.

- Employees are responsible for exercising good judgment regarding the reasonableness of use.
- Employees should take all necessary steps to prevent unauthorized access to confidential data which includes sensitive information.
- Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts.
- All PCs, laptops and workstations should be secured with a password-protected screensaver with the automatic activation feature.
- All POS and PIN entry devices should be appropriately protected and secured so they cannot be tampered or altered.
- Information contained on portable computers is especially vulnerable, special care should be exercised.

## Protect Stored Data

- All sensitive information stored and handled by the Company and its employees must be securely protected against unauthorised use at all times. Any sensitive information that is no longer required by the Company for business reasons must be discarded in a secure and irrecoverable manner.
- If there is no specific need to see the full PAN (Permanent Account Number), it has to be masked when displayed.
- PAN'S which are not protected as stated above should not be sent to the outside network via end user messaging technologies like chats, ICQ messenger etc.,
- If a client wishes to have the sensitive information removed and destroyed.

**It is strictly prohibited to store:**

1. **The contents of the payment card magnetic stripe (track data) on any media whatsoever.**
2. **The CVV/CVC (the 3 or 4 digit number on the signature panel on the reverse of the payment card) on any media whatsoever.**
3. **The PIN or the encrypted PIN Block under any circumstance.**

## Physical Security

Access to sensitive information in both hard and soft media format must be physically restricted to prevent unauthorised individuals from obtaining sensitive data.

- Media is defined as any printed or handwritten paper, received faxes, floppy disks, back-up tapes, computer hard drive, etc.
- Media containing sensitive information must be handled and distributed in a secure manner by trusted individuals.
- Visitors must always be escorted by a trusted employee when in areas that hold sensitive information
- Procedures must be in place to help all personnel easily distinguish between employees and visitors, especially in areas where cardholder data is accessible. “Employee” refers to full-time and part-time employees, temporary employees and personnel, and consultants who are “resident” on Company sites. A “visitor” is defined as a vendor, guest of an employee, service personnel, or anyone who needs to physically enter the premises for a short duration, usually not more than one day.
- Personnel using the devices should be trained and aware of handling the POS devices
- All computer that store sensitive information must be password protected to prevent unauthorised use.

## Protect Data in Transit

All sensitive cardholder data must be protected securely if it is to be transported physically or electronically.

- Card holder data (PAN, track data, etc.) must never be sent over the internet via email, instant chat or any other end user technologies.
- The transportation of media via Email, containing sensitive information must only be sent using the secured CK Clinic web mail.

## Disposal of Stored Data

- All data must be securely disposed of when no longer required by the Company, regardless of the media or application type on which it is stored.
- All hard copies of sensitive information must be manually destroyed when no longer required for valid and justified business reasons.
- The Company will have procedures for the destruction of hardcopy (paper) materials. These will require that all hardcopy materials are crosscut shredded, incinerated or pulped so they cannot be reconstructed.
- The Company will have documented procedures for the destruction of electronic media.
- All cardholder information awaiting destruction must be held in lockable storage containers clearly marked “To Be Shredded” - access to these containers must be restricted.

## Transfer of Sensitive Information Policy

- All third-party companies providing services to the Company must provide an agreed Service Level Agreement in connjunction with The Company policy

## User Access Management

- Access to Company is controlled through a formal user registration process beginning with a formal notification from HR or from a line manager.
- Each user is identified by a unique user ID so that users can be linked to and made responsible for their actions. The use of group IDs is only permitted where they are suitable for the work carried out.
- There is a standard level of access; other services can be accessed when specifically authorized by HR/line management.
- The job function of the user decides the level of access the employee has to cardholder data

- A request for service must be made in writing (email or hard copy) by the newcomer's line manager or by HR. The request is free format, but must state:

    4. Name of person making request;
    5. Job title of the newcomers and workgroup;
    6. Start date;
    7. Services required (default services are: MS Outlook, MS Office and Internet access).

- Each user will be given a copy of their new user form to provide a written statement of their access rights, signed by an IT representative after their induction procedure. The user signs the form indicating that they understand the conditions of access.
- Access to all the Company systems is provided by IT and can only be started after proper procedures are completed.

- As soon as an individual leaves the Company employment, all his/her system logons must be immediately revoked.
- As part of the employee termination process HR (or line managers in the case of contractors) will inform IT operations of all leavers and their date of leaving.
    8.
    9.

### Access Control Policy

10.

- Access Control systems are in place to protect the interests of all users of the Company computer systems by providing a safe, secure and readily accessible environment in which to work.
- The Company will provide all employees and other users with the information they need to carry out their responsibilities in an as effective and efficient manner as possible.
- Generic or group IDs shall not normally be permitted, but may be granted under exceptional circumstances if sufficient other controls on access are in place.
- The allocation of privilege rights (e.g. local administrator, domain administrator, super-user, root access) shall be restricted and controlled, and authorization provided jointly by the system owner and IT Services. Technical teams shall guard against issuing privilege rights to entire teams to prevent loss of confidentiality.
- Access rights will be accorded following the principles of least privilege and need to know.
- Every user should attempt to maintain the security of data at its classified level even if technical security mechanisms fail or are absent.
- Users electing to place information on digital media or storage devices or maintaining a separate database must only do so where such an action is in accord with the data's classification.
- Users are obligated to report instances of non-compliance to the Company CISO.
- Access to the Company IT resources and services will be given through the provision of a unique Active Directory account and complex password.
- No access to any the Company IT resources and services will be provided without prior authentication and authorization of a user's the Company Windows Active Directory account.
- Password issuing, strength requirements, changing and control will be managed through formal processes. Password length, complexity and expiration times will be controlled through Windows Active Directory Group Policy Objects.
- Access to Confidential, Restricted and Protected information will be limited to authorised persons whose job responsibilities require it, as determined by the data owner or their designated representative. Requests for access permission to be granted, changed or revoked must be made in writing.
- Users are expected to become familiar with and abide by the Company policies, standards and guidelines for appropriate and acceptable usage of the networks and systems.
- Access for remote users shall be subject to authorization by IT Services and be provided in accordance with the Remote Access Policy and the Information Security Policy. No uncontrolled external access shall be permitted to any network device or networked system.
- Access to data is variously and appropriately controlled according to the data classification levels described in the Information Security Management Policy.
- Access control methods include logon access rights, Windows share and NTFS permissions, user account privileges, server and workstation access rights, firewall permissions, IIS intranet/extranet authentication rights, SQL database rights, isolated networks and other methods as necessary.

- A formal process shall be conducted at regular intervals by system owners and data owners in conjunction with IT Services to review users' access rights. The review shall be logged and IT Services shall sign off the review to give authority for users' continued access rights.