Data Protection Policy

MedCred

Version 1.1

This policy may be updated at any time without notice to ensre changes to MedCred organisation structure are properly reflected in the policy. Please ensure you check MedCred website for the most up to date version of this policy

1. Document Information

Title:	MedCred Personal Data Protection Policy
Purpose:	To provide clear guidance and to set out the requirements of MedCred relating to the protection of personal data.
Author:	**Shokri Raoof**
Publication date:	**April 2020**
Target Audience:	All MedCred staff, students, interns and work experience candidates, contractors, sub-contractors, agency staff, medical colleges and authorised third party commercial service providers
Superseded Documents: **Related Documents:**	
Review Date:	**April** 2020
Contact Details **Data Protection Officer** **MedCred**	Email: shokriar@raoofconsultancy.com Phone: 0866047252

2. Document History

Version	Owner	Author	Publish Date
1.0	MedCred	Shokri Raoof	April 2020
1.1	MedCred	Shokri Raoof	April 2020

Contents

3. Purpose/Overview

MedCred must comply with all applicable data protection, privacy and security laws and regulations (collectively referred to as requirements) in the locations in which we operate. Through maintaining a high standard of data protection MedCred wants to foster a culture that is honest, compassionate, transparent and accountable.

The objective of this Data Protection Policy is to set out the requirements of MedCred relating to the protection of personal data where we act as a Data Controller and / or Data Processor, and the measures we will take to protect the rights of data subjects, in line with EU and Irish legislation.

In the course of our work, we are required to collect and use certain types of information about people (hereafter referred to as data subjects in line with the regulation), inclXding µpersonal data¶ as defined by the General Data Protection Regulation (GDPR). This information can relate to patients, service users, current, past and prospective employees, suppliers and others with whom staff communicate. In addition, staff may occasionally be required to collect and use certain types of personal information to comply with the requirements of other legislation for example infectious diseases legislation and the National Cancer Registry. This document sets out to ensure compliance with the GDPR.

4. Scope

This policy applies to all MedCred staff, students, interns and work experience candidates, contractors, sub-contractors, agency staff and authorised third party commercial service providers and other persons or entities when receiving, handling or processing personal data as defined by the GDPR.

This policy should be read and implemented in conjunction with MedCred Data Governance policy, which is currently under development. This policy applies to all forms of data including computer, manual and CCTV records relating to citizens.

5. Definitions

A list of terms used throughout this policy are defined in Appendix A.

6. Policy

It is the policy of MedCred that all data is processed and controlled in line with the principles of the GDPR and relevant Irish legislation.

6.1 Data Protection Principles

The following data protection requirements apply to all instances where personal data is stored, transmitted, processed or otherwise handled, regardless of geographic location.

MedCred will comply with the following high level principles:

- Personal data shall only be processed fairly, lawfully and in a transparent manner (Principles of Lawfulness, Fairness and Transparency);
- Personal data shall be obtained only for specified, explicit, lawful, and legitimate purposes, and shall not be further processed in any manner incompatible with those purposes (Principle of Purpose Limitation);

- Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (Principle of Data Minimisation);
- Personal data shall be accurate, and where necessary kept up to date (Principle of Accuracy);
- Personal data shall not be kept for longer than is necessary for the purposes for which the personal data are processed (Principle of Data Storage Limitation); Personal data will be retained in line with MedCred data retention policies.
- Personal data shall be processed in a secure manner, which includes having appropriate technical and organisational measures in place to:

    i. prevent and / or identify unauthorised or unlawful access to, or processing of, personal data; and
    ii. prevent accidental loss or destruction of, or damage to, personal data (Principles of Integrity and Confidentiality)

MedCred shall be responsible for, and be able to demonstrate compliance with, these key principles. (Principle of Accountability)

In addition, MedCred will ensure that data subject's rights are protected as set out in the GDPR.

- Data subjects will be able to request access to data we hold on them through a Subject Access Request (SAR) (Right of Access);
- Data subjects can request to change or correct any inaccurate data (Right to Rectification);
- Data subjects have the right to object to having their data processed (Right to Restriction of Processing);
- Data subjects can request to delete data that we hold excluding medical records(Right to Erasure (sometimes referred to as the Right to be Forgotten));
- Data subjects can request to have their data moved outside of MedCred if it is in an electronic format (Right to Data Portability);
- Data subjects can object to a decision made by automated processing, with certain limited exceptions (such as legitimate grounds for the processing or the defence of legal claims) and request that any decision made by automated processes have some human element (Right to Object to Automated Decision Making, including Profiling).

6.2 Data Processing Policy Requirements

MedCred, as a Data Controller, shall be responsible for, and be able to demonstrate compliance with these GDPR Requirements.

- We will process personal data in accordance with the rights of data subjects.
- We will communicate with data subjects in a concise, transparent, intelligible and easily accessible form, using clear language.
- We will only transfer personal data to Third Parties within Ireland and outside of the European Economic Area (EEA) in accordance with this policy.
- We shall conduct all personal data processing in accordance with legitimate GDPR based processing conditions in particular;
    - Data subject consent for one or more specific purposes not covered under the processing of special categories of personal data.
      or
    - Necessary processing for contract performance or contract entry.
      or
    - Legal obligation underpinning processing.

6.3 Processing of Special Categories of Personal Data

Special categories of data are defined by the GDPR and include data such as racial or ethnic origin, religious or philosophical beliefs, genetic data, biometric data, health data, sex life details and sexual orientation.

If the processing of data is not covered by the categories above MedCred will require explicit consent f rom the data subject.

6.4 Processing of Personal Data

1. The processing is necessary in order to protect the vital interests of the person (referred to as the data subject in Data Protection language).
2. The processing is necessary for a task carried out in the public interest or in the exercise of official authority vested in the controller; for MedCred this official authority.
3. Processing of personal data is permitted where is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.

6.5 Data Storage Limitation Policy

MedCred should erase any personal data that violates;

- Data Protection Law
- Data Protection Regulations
- Contractual Obligations
- Requirements of this Policy
- If MedCred no longer requires the Data

6.6 Data Anonymisation and Pseudonymisation

MedCred must anonymise and / or pseudonymise personal data when it is being used for purposes other than the direct provision of public health and health and social care services.

6.7 Information Security

All MedCred staff must familiarise themselves with the up to date information security policies.

6.8 Unauthorised Disclosure

All persons covered under this policy are prohibited from disclosing a data subject¶s confidential information (including personal data or special categories of personal data), unless this policy or a legal basis allows for such disclosures.

All persons covered under this policy must report all suspected incidents of unauthorised access to the relevant deputy DPO office. Incidents include disclosure, loss, destruction or alteration of patient and serYice Xser¶s personal information, regardless of whether it is in paper or electronic form.

MedCred has established formal procedures for reporting suspected incidents of unauthorised disclosure of data. All persons covered under this policy must follow these procedures which can be found at http://MedCred.org

6.9 Privacy by Design, Data Protection by Design & Data Protection by Default Policy

MedCred aims to use its systems and processes which are guided by strict adherence to data protection legislation in the delivery of health and social care services.

Aside from general data protection policy we must incorporate the following principles in projects involving the design of a new or changing an existing service.

- Privacy by Design and by Default
- Data Protection by Design and by Default

If any staff member considers that particular class of personal data processing may affect a data subject¶s rights and freedoms then they should;

- Engage the DPO or deputy DPO in terms of the issue.
- Conduct a mandatory Data Protection Impact Assessment (DPIA).

All Data Protection Impact Assessments must be registered with the DPO office.

6.10 Third Party Transfer Policy

MedCred must not transfer personal data to a Third Party outside of the EEA regardless of whether MedCred is acting as a Data Controller or Data Processor unless:

- The EU recognises the transfer country/territory as having an adequate level of data subject legal protection relating to personal data processing or
- The EU recognises the transfer mechanism as providing adequate protection when made to countries/territories lacking adequate legal protection. Please see https://www.dataprotection.ie/docs/Transfers-Abroad/1244.htm
- The explicit consent of the data subject is required to allow Third Party transfer or transfer is authorised by law.
- All reasonable, appropriate and necessary steps have been taken to maintain the required level of Personal data Protection; and

Subject to the provisions above, including any necessary MedCred approvals, MedCred may transfer personal data to a Third Party outside of the EEA where any of the following apply:

- The transfer is necessar\ to protect the data sXbject¶s Yital interests; or
- The data subject has given explicit consent to the proposed transfer; or
- The transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between MedCred and a Third Party; or

- The transfer is necessary or legally required for the establishment, exercise, or defence of legal claims; or
- The transfer is required by law; or
- The transfer is made from a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest.

The DPO must assess whether any of the above exceptions apply prior to any personal data transfer and must record the determination in writing.

6.11 Third Parties Relationships Policy

Where MedCred engages a Third Party for processing activities, this Data Processor must protect personal data through sufficient technical and organisational security measures and take all reasonable GDPR compliance steps.

When engaging a Third Party for personal data processing, MedCred must enter into a written contract, or equivalent. This contract or equivalent shall:

- Clearly set out respective parties responsibilities
- Must ensure compliance with relevant European and local Member State Data Protection requirements/legislation.
- At the expiry of a data processor contract the data processor is contractually obliged to return the full dataset to MedCred and provide unequivocal evidence that their copy of the dataset is erased.

MedCred must ensure that all Third Party relationships are established and maintained. Data processors who are processing data on behalf of MedCred must secure approval from MedCred if they wish to engage further data processors

6.12 Education and Awareness Policy

MedCred will ensure that data protection training material is available through MedCredLand (The MedCred e-learn environment). In addition to General Data Protection Regulation training staff may receive additional training when applicable to their duties or position.

7. Roles and Responsibilities

7.1 Office of the Data Protection Officer

The data protection officer (DPO) and deputy data protection officers should be involved, properly and in a timely manner, in all issues which relate to the protection of personal data. They are bound by secrecy or confidentiality concerning the performance of their tasks, in accordance with Union or Member State law.

They are responsible for monitoring compliance with the GDPR and have overall control of how data is processed within MedCred,

This will include:

- Collecting information about processing activities
- Analysing and checking the compliance of processing activities,
- Informing, advising and issuing recommendations management and the relevant data processors and controllers
- Where a national unified or coordinated response is needed, cooperation/collaboration with other organisations DPOs may take place.

8. Enforcement

MedCred reserves the right to take such action as it deems appropriate against individuals who breach the conditions of this policy. MedCred staff who breach this policy may be subject to disciplinary action as provided for in MedCred disciplinary procedure. If a breach occurs due to reckless behaviour and a breach occurs and is knowingly not reported, the person responsible may be held accountable.

Where a breach of this policy is committed by contractors, sub-contractors, agency staff and authorised third party commercial service providers, MedCred reserves the right to remedy via the contracts in existence.

9. Review & Update

This policy will be reviewed and updated every 3 years or more frequently if necessary to ensure any changes to MedCred's organisation structure and business practices are properly reflected in the policy.

10. Appendix A - Glossary of Terms

Term	Description
Anonymised	Means the process of making personal data anonymous data. Anon\mise should be construed accordingly.
Anonymous Data	means any information relating to a natural person where the person cannot be identified, whether by the Data Controller or by any other person, taking account of all the means reasonably likely to be used either by the Data Controller or by any other person to identify that individual.
Biometric Data	means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data
Consent	Means any freely given, specific, informed and unambiguous indication of the data subject¶s Zishes b\ Zhich he or she, b\ a statement or b\ a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.
Data	as used in this Policy shall mean information which either: x is processed by means of equipment operating automatically in response to instructions given for that purpose; x is recorded with the intention that it should be processed by means of such equipment; x is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system; x Does not fall within any of the above, but forms part of a readily accessible record. x Data therefore includes any digital data transferred by computer or automated equipment, and any manual information which is part of a relevant filing system.
Data Controller	Means a person or organisation who (alone or with others) determines the purposes for which and the manner in which any personal data are, or are to be, processed. A Data Controller can be the sole Data Controller or a joint Data Controller with another person or organisation.
Data Processor	Means a person or organisation that holds or processes personal data on the instructions of the Data Controller, but does not exercise responsibility for, or control over the personal data.
Data Protection	Means the protection of personal data
Data Protection Commission	Means the office of the Data Protection Commission in Ireland.
Data subject	Refers to the individual to whom personal data held relates, including: employees, customers, suppliers.
DPO	Data Protection Officer

EEA	European Economic Area Means the area in which the Agreement on the EEA provides for the free movement of persons, goods, services and capital within the European Single Market, as well as the freedom to choose residence in any country within this area.
Encryption	It is the process of encoding information stored on a device and can add a further useful layer of security. It is considered an essential security measure where personal data is stored on a portable device or transmitted over a public network.
EU Directive	Means the EU Data Protection Directive 95/46/EC.
Genetic Data	means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question

Information Request	Means a request from a data subject relating to that individual's personal data.
Personal Data	Means any information relating to an identified or identifiable natural person (Data subject). 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 by reference to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
Processing	means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. The terms,Process and Processed should be construed accordingl\.
Pseudonymisation	Means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.
Personal Data Breach	means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed
Restriction of Processing	Means the marking of stored personal data with the aim of limiting their processing in the future.
SMT	Means the Senior Management Team/Board of MedCred.
Subject Access Request	Means a written request made to a Data Controller by any individual about whom a Data Controller keeps personal data on computer or in a relevant filing system. Response must be provided to the data subject under the terms outlined by GDPR and/or local requirements.
Third Party	Means an entity, whether or not affiliated with MedCred, that is in a contractual arrangement with MedCred. These Third Party relationships include, but are not limited to, activities that involve outsourced products and services, use of independent consultants, networking and marketing arrangements, merchant payment processing services, services provided by affiliates and subsidiaries, joint ventures and other business arrangements where MedCred has an ongoing relationship.Third Party relationships, for the purposes of this policy, generally do not include customer relationships. Under GDPR a "Third Party" means a natural or legal person, public authority, agency or body, other than the data subject, controller, processor and persons who, under the direct authority of the Data Controller of Data Processor, are authorised to process personal data.