TMC
Information Governance Policy

Security and Privacy

Document code	POL-TMC-006
Date of current document	15/05/2024
Version of the document	7.1

Index

Document Control

This document is uncontrolled when printed. Please verify that you have the most recent version of this document by contacting the Security and Quality Board.

Name of document: POL-TMC-006

Document History

(current version is on the top as version and date are repeated in the document, the previous version appears under the yellow row)

VERSION	DATE	CHANGES	AUTHOR
Current version:			
7.1	15/05/2024	Changed address of TMC Australia	Ida Anderman
Older versions (write, don't copy from above):			
1.0	24.09.2008	Draft	Ida Anderman
2.0	15.10.2008	Document approved	Ida Anderman
2.1 to 6.4		See intranet version history	
6.5	02/12/2020	Update with ISO 27701 requirements	Ida Anderman
6.6	15/02/2021	Updated address of UK entity	Ida Anderman
6.7	20/01/2022	Updated address of BCN and UK entity Referenced new Business Continuity Strategy policy	Ida Anderman
6.8	04/01/23	Yearly review	Ida Anderman
6.9	30/01/2023	Added Cybersecurity to the list of responsibilities of the ISMS Manager	Javier Castillo
7.0	14/07/2023	Added Contact details, detailed rights of data subjects and a note about TMC entities.	Ida Anderman

Date of document review: Before end of March every year or at times of relevant changes.
Responsible department: IG Lead/ISMS Manager

Confidentiality and Non-Disclosure

This document is classified as Non-Restricted. This document and all information within this document will remain at all times the property of TMC.

Related documentation

POL-TMC-013 TMC Policy framework
POL-TMC-002 TMC Management System Manual
GDPR EUR-Lex - 32016R0679 - EN - EUR-Lex
ISO-IEC 27001.2013
iso-iec-27701-2019
SOP-ISMS-001 Statement of Applicability 27001-2013
POL-TMC-029 Unilabs Group Cybersecurity Policy
Data Processing Inventory
SOP-TMC-036 New data processing workflow
SOP-TMC-033 Data Protection by Design and by Default
SOP-TMC-041 Unilabs_Guidance on Privacy by Design by Default
SOP-TMC-034 Data Protection Breaches process
SOP-TMC-038 Unilabs - Global Data Breach Notification procedure
SOP-TMC-032 Data Subject rights process
SOP-TMC-037 Unilabs - Global Data Subject Rights Requests Handling Procedure
SOP-TMC-039 Unilabs_Data Protection Impact Assessment Guidance
SOP-TMC-035 Data Privacy Impact Assessment
SOP-TMC-040 Unilabs - Global Information Notice procedure
SOP-TMC-042 Unilabs - Guidance for Data Processing Agreements
POL-TMC-031 Unilabs Group Cybersecurity Charter
POL-TMC-030 Unilabs Group Privileged User Charter
POL-TMC-036 Unilabs - Global Data Transfer Policy
POL-TMC-033 Unilabs - Global Data Retention Policy
POL-TMC-032 Unilabs - Data Protection Governance Policy
POL-TMC-013 TMC Policy framework
POL-TMC-011 TMC Security and Confidentiality User guidelines
POL-TMC-034 Unilabs - Global GDPR Training Policy
SOP-TMC-055 TMC Protecting PII SOP
SOP-TMC-051 Accuracy of Personal data procedure
DOC-TMC-043 TMCs role as Controller and Processor
DOC-TMC-044 Scope of PIMS
POL-TMC-017 Definition and Use of Patient Identifiable Information
SOP-TMC-057 IS and Privacy Objectives
POL-TMC-039 Business Continuity Strategy

Definitions

“Information System” Includes all servers and clients, network infrastructure, systems and applications, as well as the use of all internal and external services such as Internet access, e-mail. Etc.

“ISMS” means Information Security Management system.
“ISMS” Manager means Information Security Management system manager

“Information assets” In the context of this Policy the term Information assets is applied to….

“Controller” means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.

“Data Protection Law” means all applicable legislation relating to data protection and privacy including without limitation the EU Data Protection Directive 95/46/EC and all local laws and regulations which amend or replace any of them, including the GDPR, together with any national implementing laws in any Member State of the European Union or, to the extent applicable, in any other country, as amended, repealed, consolidated or replaced from time to time. The terms “process”, “processes” and “processed” will be construed accordingly.

“Data Subject” means the individual to whom Personal Data relates.

“Individual” means the individual to whom Personal Data relates.

“GDPR” means the General Data Protection Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons regarding the processing of personal data and on the free movement of such data.

“Instruction” means the written, documented instruction, issued by Controller to Processor, and directing the same to perform a specific action regarding Personal Data (including, but not limited to, depersonalizing, blocking, deletion, making available).

“Personal Data” means any information relating to an identified or identifiable individual where such information is contained within Customer Data and is protected similarly as Personal Data or personally identifiable information under applicable Data Protection Law

“Special Category Data” is information relating to; - racial or ethnic origin, political opinions, religious or other beliefs, trade union membership, genetic data, biometric data, a person’s age, data concerning health, data concerning a natural person’s sex life or sexual orientation.

“Personal Data Breach” means a breach or incident of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise processed.

“Processing” means any operation or set of operations which is performed on Personal Data, encompassing the collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction or erasure of Personal Data.

“Processor” means a natural or legal person, public authority, agency or other body which processes Personal Data on behalf of the Controller.

“Standard Contractual Clauses” means the clauses attached hereto as Exhibit 1 pursuant to the European Commission’s decision (C(2010)593) of 5 February 2010 on Standard Contractual Clauses for the transfer of Personal Data to processors established in third countries which do not ensure an adequate level of data protection.

”Caldicott Guardian” is an NHS (UK) appointee who is responsible for policies that safeguard the confidentiality and security, information clarity, rights of access and documentation

accuracy of patient data. Caldicott Guardians are often senior professionals working within a particular NHS organisation-trust or in general practice.

”IG lead” mean Information Governance Lead

”SIRO” means Senior Information Risk Owner, a role defined by the Data Protection Security Toolkit. The Senior Information Risk Owner (SIRO) should be an Executive Director or other senior member of the Board (or equivalent senior management group/committee).
The SIRO may also be the Chief Information Officer (CIO) if the latter is on the Board, but should not be the *Caldicott Guardian* as the SIRO should be part of the organisation's management hierarchy rather than being in an advisory role.

”SQB” means TMC Security and Quality Board

”DPO” means Data Protection Officer
“PIMS” means Privacy Information Management System. It is the information security management system that addresses the protection of privacy as potentially affected by the processing of personal data (PII)

“Privacy Information Management System”, see “PIMS”

“Customer” or “Client” means:
Depending on the role of the organisation (Controller or Processor) “customer” can be understood as :

a) An organisation who has a contract with a PII controler (e.g. the customer of the PII controller)
b) A PII controller who has a contract with a PII processor (e.g. the customer of the PII processor)
c) A PII processor who has a contract with a subcontractor for PII processing (e.g. the customer of the subcontracted PII sub-processor).

“Personally identifiable information (PII)” means ‘Personal Data’ in the GDPR. ISO 29100 defines this as “information that (a) can be used to identify the PII principal to whom such information relates, or (b) is or might be directly or indirectly linked to a PII principal” (Clause 2.9).

“PII principal” means ‘data subject’ in the GDPR. ISO 29100 defines this as a “natural person to whom the personally identifiable information (PII) relates” (Clause 2.11).

“PII controller” means ‘data controller’ in the GDPR. ISO 29100 defines this as the “privacy stakeholder (or privacy stakeholders) that determines the purposes and means for processing personally identifiable information (PII) other than natural persons who use data for personal purposes” (Clause 2.10).

“Joint PII controller” means entities that jointly determine the “means and purposes” of the processing are joint controllers. The participation of parties in the determination of purposes and means of processing in the context of joint control may take different forms and does not need to be equally shared. (Clause 7.2.7 Joint PII Controller)

“PII processor means ‘data processor’ in the GDPR. ISO 29100 defines this as the “privacy stakeholder that processes personally identifiable information (PII) on behalf of and in accordance with the instructions of a PII controller” (Clause 2.12).

To clarify - terms used by TMC:

Privacy and Data Protection has the same significance in this policy and are both used.
Data Subject, Individual and **PII Principal** means the natural person to whom the personally identifiable information (PII) relates. Both terms are used and have the same meaning in this policy.
Personally identifiable information (PII)" means 'personal data' and both terms have been used in this policy with the same meaning.

Contact details for Data Protection topics or complaints

If we are processing your data:
You as an individual, have the following rights:

- A right to receive certain information about our Processing activities in a concise, transparent, intelligible and easily accessible form, using clear and plain language;
- A right of access that you may exercise by asking a copy of your personal data;
- A right to correct your personal data if they are inaccurate or incomplete and a right to obtain the restriction of the processing of your personal data;
- A right to erase your personal data, in cases where your personal data are processed on the basis of your consent, the performance of a contract to which you are party and our legitimate interests;
- A right to data portability, in cases where your personal data are processed on the basis of your consent and/or the performance of a contract to which you are party;
- A right to object, on grounds relating to your particular situation, to the processing of your personal data in cases where your personal data are processed on the basis of our legitimate interests.
- The right to restrict processing in certain specific circumstances (for example where the accuracy of the personal data is contested by the data subject);
- The right to object in certain specific circumstances (for example to the processing for direct marking purposes);
- Right in relation to automated decision making and profiling;
- Right to Withdraw Consent;

If you want to exercise your rights you should contact TMC by means of an email to dataprotection@telemedicineclinic.com or in writing to C/ Marina, 16-18, Pl. 33, 08005, Barcelona, Spain providing a copy of your Identification card, and indicating the full address - email with the purposes of notifications related to the requests from TMC, and specifically pointing out the data on which the right in question exercises. However, you are hereby informed that the exercise of some of the abovementioned privacy rights could hinder or impede the performance of the purposes before indicated.

Right to lodge a complaint with the Data Protection Authority
You have also the right to lodge a complaint with a Data Protection Authority, either in the Member State of your habitual residence, place of work or place of an alleged infringement of the data protection laws.

In Spain, this is the “AEPD”.
In the United Kingdom, the “ICO”.
In Denmark, the “Datatilsynet”.
In Sweden, the "IMY”.
In Norway, the “Datatilsynet”.

Contact details of the Data Protection Officer (DPO) and the Local Data Protection Coordinators
The TMC – Unilabs DPO can be contacted in writing: dpo@unilabs.com

The team who is managing Data Protection topics on a daily basis in TMC are the Local Data Protection Coordinators.

- Ida Anderman
- Edona Mehmeti

They can be contacted by email: dataprotection@telemedicineclinic.com

1. Introduction

This top-level Information Security and Privacy Policy is a key component of TMC overall Information Security management framework and should be considered alongside more detailed Information Security documentation, including system level security policies, security guidance and protocols or procedures.

This policy also covers Privacy and Data Protection.
TMC needs to gather and process certain information about individuals (Personal Data/ PII). Such individuals may include employees, customers, suppliers and other people the organisation has a relationship with or may need to contact.
This policy describes how this personal data must be collected, handled and stored to the requirements of the General Data Protection Regulations and in line with ISO 27001 and ISO 27701.
This Policy should be read in conjunction with TMC´s Privacy Statements on the main website: https://www.telemedicineclinic.com/data-protection/

2. Objectives

The objectives of TMC Information Security and Privacy Policy are to preserve:

- **Confidentiality** - Access to Data shall be confined to those with appropriate authorization.
- **Integrity** – Information shall be complete and accurate. All systems, assets and networks shall operate correctly, according to specification.
- **Availability** - Information shall be available and delivered to the right person, at the time when it is needed.

3. Policy aim

The aim of this policy is to establish and maintain the security and confidentiality of information, information systems, applications and networks owned or held by TMC by:

- Ensuring that all members of staff are aware of and fully comply with the relevant legislation as described in this and other policies and follows good practice.
- Describing the principals of security and explaining how they shall be implemented in the organisation.
- Introducing a consistent approach to Security and Privacy, ensuring that all members of staff fully understand their own responsibilities.
- Creating and maintaining within the organisation a level of awareness of the need for Information Security and Privacy as an integral part of the day to day business.
- Protecting information assets under the control of the organisation.
- Protecting the rights of employees, customers and business partners
- Being open about how it stores and processes individual data
- Minimising the risks of a data breaches
- Demonstrate the commitment from TMC Senior Leadership Team to satisfy privacy requirements.

4. Commitment Statements

TMC has documented the general commitment to meet standards and regulations in the Framework policy that covers Quality, Information Security and Privacy. It can be accessed on the TMC website and intranet: https://www.telemedicineclinic.com/quality/
And in POL-TMC-013 TMC Policy framework

The Privacy statement is available on the website:
https://www.telemedicineclinic.com/data-protection/

5. Scope

The scope of the TMC Information Management System of Information Security services is ***"Medical diagnostic services in teleradiology and medical training".***

Companies covered of the Management System are:

European Telemedicine Clinic S.L.
Torre Mapfre
C/Marina 16-18,
33rd Floor
08005 Barcelona, Spain

Telemedicine Clinic Ltd
Visiting office:
Davidson House, Forbury Square,
Reading, RG1 3EU
The company is registered in:
2 Chamberlain Square,
Birmingham , B3 3AX, UK

Australian Telemedicine Clinic Pty
Level 63,
25 Martin Place,
Sydney NSW 2000, Australia

Other entities of TMC need to meet the same standards as the above mentioned entities and in scope for this policy but are not included in the ISO 27001 Scope.

This policy covers all information within the organisation, including (but not limited to):

- Patient, client and service user information (for further details refer to the company Security Document)
- Staff, contractor and volunteer information (for further details refer to the company Security Document)
- Financial information
- Management information

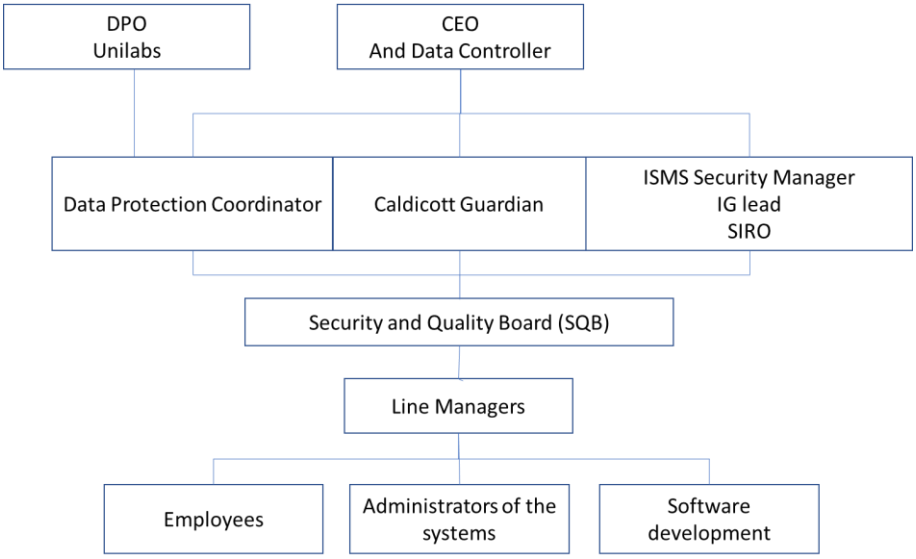
This policy covers all information, no matter what form it is stored or used in, including (but not limited to):

- Structured record systems - paper and electronic
- Unstructured record systems – paper and electronic

- Transmission of information – fax, e-mail, post and telephone

The scope of TMC´s Personal Information Management System (PIMS) consists of the above. DOC-TMC-044 Scope of PIMS

6. Responsibilities for Information Security and Data Protection



6.3 Ultimate responsibility for Information Security and Privacy rests with the TMC Chief Executive Officer and the Senior Leaderhship team (SLT) but on a day-to-day basis other profiles shall be responsible for managing and implementing the policy and related procedures. They delegate responsibilities and authorities to managers and individuals to ensure that Information Security and Privacy management systems conform to regulations, best standards and requirements of ISO 27001 and ISO 27701.

6.4 The Data Protection Officer (DPO) on Unilabs group level is supporting the local TMC Information Security and Privacy organisation with data subject requests, doubts, data breach management. The DPO reports to the Finance department in Unilabs and to the Group Executive Management and the Data Protection Core Team. This is described in detail in the Unilabs Global Data Protection Governance Policy.

6.5 The Data Protection Coordinator (DP Coordinator) ensures that the TMC group complies with GDPR and local data protection laws. Provides training and support and is the main contact with the Unilabs Group DPO and the managers involved in Data Protection

6.6 TMC has appointed their Head of IT as Information Security Management System Manager (also called ISMS Manager). The UK NHS Digital Data Protection and Security Toolkit roles “IG lead” and “SIRO” are also performed by the Head of IT. The ISMS Manager is responsible for the security administration within the TMC organisation, ensuring that appropriate technical and organisational measures are in place to preserve confidentiality, integrity, availability of the data processed by TMC. The ISMS Manager is also responsible for the PIMS and cybersecurity.

6.7 The “Caldicott Guardian” role is performed by the Medical Director. This role exists within the NHS in the UK and is a senior medical staff member whose main responsibility is to ensure patient data is kept secure.

6.8 The TMC Security and Quality Board (SQB), led by the Quality Manager, consists of selected managers and key employees who all act as Security officers. This board is both providing advise related to quality and security as well as implementing, monitoring, documenting and communicating security requirements in the organisation.

6.9 Line Managers[1] are responsible for ensuring that their permanent and temporary staff and contractors are aware of: -

- The Information Security policies applicable in their work areas
- Their personal responsibilities for Information Security
- How to access advice on Information Security matters
- Ensure the staff members follow TMC and Unilabs guidelines and this policy.

6.10 All staff shall comply with Information Security procedures including the maintenance of data confidentiality and data integrity. Failure to do so may result in disciplinary action.

6.11 The Information Security Policy shall be maintained, reviewed and updated by the TMC Security and Quality Board. This review shall take place annually. The CEO or the Information Security Management manager should sign the policy.

6.12 Line managers shall be individually responsible for the security of their physical environments where information is processed or stored.

6.13 Each member of staff shall be responsible for the operational security of the information systems they use.

6.14 Each system user shall comply with the security and privacy requirements that are currently in force, and shall also ensure that the confidentiality, integrity and availability of the information they use are maintained to the highest standard.

6.15 Contracts with external contractors that allow access to the organisation's information systems shall be in place before access is allowed. These contracts shall ensure that the staff or sub-contractors of the external organisation shall comply with all appropriate security and privacy policies.

6.16 Yearly, or more frequently if deemed necessary, the TMC Security and Quality Board will send out a reminder email to all staff explaining changes or new needs, requirements, legislation, policies or procedures, etc. concerning Information Security and Privacy. This is scheduled via IT Periodic task.

6.17 TMC SLT must ensure that all staff are aware that when they process health data, they must treat such data confidentially. This is legally binding and covers all staff with access to the patients' health records.

6.18 TMC SLT assigns responsibilities and authorities for reporting on performance of the Management systems related to Information Security and Privacy. A yearly report on GDPR and Information Security compliance should be produced by the ISMS manager and the DP Coordinator and sent to SLT for review.

6.19 Responsibilities are further described in individual job descriptions.

POL-TMC-032 Unilabs - Data Protection Governance Policy
POL-TMC-029 Unilabs Group Cybersecurity Policy
POL-TMC-002 TMC Management System Manual

[1] Also called Business Referents (see Unilabs Data Protection Governance Policy), one in each department of Operations, IT, Sales, Marketing and Communication, Procurement, Finance and Compliance.

POL-TMC-017 Definition and Use of Patient Identifiable Information (Describes the role of the Caldicott Guardian and Caldicott principles)

7. Legislation & 3rd Party requirements

TMC is obliged to abide by relevant UK and European Union legislation and the legislations in the clients' countries and the countries where the TMC offices are located. The requirement to comply with this legislation shall be devolved to employees and consultants of TMC, who may be held personally accountable for any breaches of Information Security and Privacy for which they may be held responsible. When it comes to the security of patient data, it is a requirement that the clients provide TMC with the instructions for how they, as data controllers of the data, expect the data to be treated, via the contractual/confidentiality agreement.

8. Policy Framework

This policy has been updated in accordance with what is stipulated in the EU regulation (UE) 2016/679 approved by the EU Parliament on 14 April 2016 (GDPR) and relevant national data protection law in the countries where we operate.

The Regulations describe how organisations, including Telemedicine Clinic, must collect, access, organise, store and destroy personal data (i.e. Processing).
Not only must the Company comply with the law regarding the processing of personal data safely and lawfully, the Company must demonstrate its compliance with the law.

The rules apply regardless of whether data is stored electronically, on paper or on other materials (e.g. CCTV)

The General Data Protection Regulations are underpinned by the following important principles; -

- **Lawfulness, fairness and transparency:**
  Personal data must be processed lawfully, fairly and in a transparent manner in relation to the data subject.

- **Purpose Limitation:**
  Personal data must be collected only for specified, explicit and legitimate purposes.

- **Data Minimisation:**
  Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.

- **Accuracy:**
  Personal data must be accurate and where necessary kept up to date.

- **Storage Limitation:**
  Personal data which is kept in a form which permits identification of data subjects must be kept for no longer than is necessary for the purpose for which data is processed.

- **Integrity and Confidentiality:**

Personal data must be processed in a manner that, through use of technical or organisational measures, ensures appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.

- **Accountability:**
  The data controller is responsible for and must be able to demonstrate compliance with the other data protection principles.

Additionally, we comply with the following Privacy principles:

- **Consent and choice:**
  The individuals should have the choice whether to allow their data to be processed or not
- **Individual participation and access:**
  Individuals should be able to access and review personal data, as permitted by the law
- **Information Security:**
  There should be controls in place to protect the confidentiality, integrity and availability of the personal data

TMC is also complying with ISO 27001 and ISO 27701 (see certificates on https://www.telemedicineclinic.com/quality/), which are standards that provide guidance and best practice of Information Security and Privacy and how to handle data security risks.

TMC complies with all the above in the following way:

8.3 Information Security and Privacy governance

- TMCs has defined the organisation structure for Information Security and Privacy, as described in this policy (see above “Responsibilities for Information Security”) and in the Unilabs Group Data Protection Governance Policy and in the Unilabs Group Cybersecurity policy.
  POL-TMC-032 Unilabs - Data Protection Governance Policy
  POL-TMC-029 Unilabs Group Cybersecurity Policy

8.4 Related processes

- TMC plans, implements and controls the processes necessary to meet information security and privacy requirements.
- These processes are described below.

8.5 Policy Audit

- Compliance with this Information Security policy will be monitored through audits.
- Yearly external audits of ISO 27001 and ISO 27701 take place.
- Internal audits are run regularly
- Business continuity and service continuity audits are done, as well as penetration tests.
- The schedule of audits and the results will be defined, reviewed and monitored by the SQB.

  SOP-TMC-007 General quality and security internal audits

8.6 Information Security Awareness Training

- Information Security and data protection awareness training shall be included in the staff induction process.

- An ongoing awareness programme shall be established and maintained to ensure that staff awareness is refreshed and updated as necessary.

- All TMC staff members and consultants need to read and agree to TMC Security and Confidentiality User guidelines, which is a comprehensive guideline about our security and how they, as users, should process and manage the data. POL-TMC-011 TMC Security and Confidentiality User guidelines

- All staff are also required to read and agree to the Cybersecurity rules presented in POL-TMC-031 Unilabs Group Cybersecurity Charter - Booklet
  POL-TMC-034 Unilabs - Global GDPR Training Policy

8.7 Risk Assessment

- TMC has adopted a systematic approach to Information Security and Privacy risk management.

- The core principle of risk assessment and management requires the identification and quantification of Information Security and Privacy risks in terms of their perceived value of asset, severity of impact and the likelihood of occurrence.

- Once identified, Information Security and Privacy risks shall be managed on a formal basis. They shall be recorded within a baseline risk register and action plans shall be put in place to effectively manage those risks. The risk register and all associated actions shall be reviewed at regular intervals. Any implemented Information Security and Privacy arrangements shall also be a regularly reviewed feature of a TMC risk management programme. These reviews shall help identify areas of continuing best practice and possible weakness, as well as potential risks that may have arisen since the last review was completed.

- In cases where the data processing activity is likely to result in a high risk for the rights of individuals, controllers must carry out a Data Protection Impact Assessment (DPIA) prior to any such processing[2]. The purpose of the assessment when performing a DPIA is for the controller* to identify and mitigate the risks. This is described in TMC-SOP-035 Data Protection Impact Assessment procedure.

  SOP-TMC-056 Privacy risk assessments and register
  Privacy risk register
  POL-TMC-025 Risk Management Strategy and Policy
  SOP-TMC-016 Risk Analysis Assessment of IT assets
  SOP-TMC-039 Unilabs_Data Protection Impact Assessment Guidance
  SOP-TMC-035 Data Privacy Impact Assessment

[2] A DPIA* must be performed in the following cases:
i) In case of systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing*, including profiling*, and on which decisions are based that produce legal effects concerning the individual or similarly significantly affect the individual;
ii) In case of processing* on a large scale of special categories of data (i.e. data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, genetic data, biometric data or data concerning health or sex life) or of data relating to criminal convictions and offences
iii) In case of a systematic monitoring of a publicly accessible area on a large scale (e.g. implementation of a CCTV system)

8.8 Continual improvement

- SLT and the SQB team define objectives related to Information Security and Privacy. These objectives are documented, actions are performed to improve the objectives, and KPIs are used to measure them. These objective are documented in SGSI-FSGSI06-V1R0-IndicadoresDeSeguridad, Security and Privacy Objectives and explained in SOP-TMC-057 IS and Privacy Objectives and the SOP-TMC-008 Process improvement

- Improvements may be detected through Risk assessments, data breaches, audits, planning and analysis of new processes and systems.

- The SQB team shall ensure actions are taken to continuously improve the company's Information Governance structure. Actions will either be listed on the company Form - CAPA Log list, IT Risk assessments and improvement lists or in the Privacy risk register

- Actions are controlled and reviewed regularly.

8.9 Contracts of Employment

- Staff security requirements shall be addressed at the recruitment stage and all contracts of employment shall contain an Information Security and confidentiality clause.

- Information Security expectations of staff shall be included within appropriate job definitions.

8.10 Legal ground for processing data

- TMC must define the legal ground for each of the data processing activities. This is specified in the SOP-TMC-036 New data processing workflow
  The legal grounds for each processing activity is documented in the Data Processing Inventory

  The legal grounds comprise;

  - **Performance of a Contract:**
    Where the organisation has a contract with an individual and needs to process their Personal data to comply with its obligations under the contract.

  - **Legal Obligation:**
    Where the organisation needs to process an individual's personal data to comply with a common law or statutory obligation.

  - **Consent:**
    Where the individual gives their consent. This must be freely given, specific, informed and unambiguous.

  - **Legitimate Interest:**
    Where the organisation identifies a legitimate interest in in "processing"
    the personal data and can show processing is necessary to achieve it. This requires the organisation to balance its needs against the interests, rights and freedoms of the individual. This is best done by completing a Privacy Impact Assessment.

  - **Vital Interest:**
    Where the organisation needs to process the individual's personal data to protect someone's life.

- **Public Task:**
  Relevant to Public bodies.

8.11 Information to Individuals

- TMC must provide information to individuals about how TMC process their personal data.

- This is done through Information Notices available on the website and provided directly to the individuals: https://www.telemedicineclinic.com/data-protection/
  SOP-TMC-040 Unilabs - Global Information Notice procedure

- The individuals can decide about their processing in all cases where TMC applies consent, for example in the case of newsletters.

8.12 The Individuals' rights

- TMC must be aware of the data subjects' rights for each data processing activity. They have the right to:
  - Be informed about how the Company will handle their data. This will normally be done by issuing an Information Notice and a Policy Statement.
  - Apply the ARCO(PE) rights:
    - Ask to gain access to personal data held about them
    - Withdraw their consent, where consent is the lawful basis for processing
    - Request their personal data is erased in certain circumstances
    - Request their personal data is transferred to a third party in certain circumstances

- There must be a process in place to manage data subjects' request to exercise their rights, including technical measures. This is documented in SOP-TMC-032 Data Subjects Rights process. The response time to answer the requests from data subjects is maximum 1 month from reception.

- The Data Processing Inventory includes information about the rights, to help guide the staff managing the requests from data subjects.

  SOP-TMC-032 Data Subject rights process
  SOP-TMC-037 Unilabs - Global Data Subject Rights Requests Handling Procedure

8.13 Data Processing Inventory

- Each data processing activity shall be registered in a Data Processing Inventory.

- The inventory needs to be regularly reviewed and updated.

- Records of processing should be available and be updated as soon as the inventory is updated.

8.14 Accuracy of data

- The organization should ensure and document that PII is as accurate, complete and up-to-date as is necessary for the purposes for which it is processed, throughout the life-cycle of the PII.
- TMC has guidelines in place for how to minimise inaccuracies in the Personal Data and mechanisms to respond in case of inaccuracies.
  SOP-TMC-051 Accuracy of Personal data procedure

8.15 Purpose limitation

TMC has documented what kind of Personal data we process and how we process it and specific requirements for each processing in the Data Processing Inventory. By adding the information to the inventory we evaluate and analyse the amount of data needed and ensure we keep it to a minimum.

When we start a new processing or make changes to how we process the personal data we need to apply the Privacy by Design and Default process, as well as, in some cases, perform Data Privacy Impact Assessments, in which we evaluate the purpose of processing, the data that is processed and what needs to be done to protect the data.
The inventory is regularly reviewed to ensure its accuracy.
SOP-TMC-036 New data processing workflow

8.16 Retention and disposal of Personal Data

TMC must either delete Personal Data or render it in a form which does not permit identification or re-identification of individuals, as soon as the original Personal Data is no longer necessary for the identified purpose(s).
TMC must ensure that temporary files created as a result of the processing of PII are disposed of (e.g. erased or destroyed) following documented procedures within a specified, documented period.
TMC must not retain PII for longer than is necessary for the purposes for which the PII is processed.

The Retention policy provides the guidance for how to do this POL-TMC-033 Unilabs - Global Data Retention Policy

The detailed retention periods for each system and processing is described in the Data Processing Inventory.

8.17 Access to personal data

The only people able to access personal data are those who need to do so for their work and should do so in accordance with one (or more) of the lawful basis identified above.

Data should not be shared informally or where there is no lawful basis, either within the Company or externally. Moreover, personal data must be held in as few places as necessary. Employees must not create unnecessary additional data sets.

The Company will at times need to process Special Category Data (or Sensitive Data). In such circumstances, the Company must identify at least one additional lawful ground (in addition to the general processing grounds, to justify processing special category data.

- Employees should keep all data secure, by taking sensible precautions. In particular strong passwords and/or encryption should be used. (See also data storage below).

- Personal data should be regularly reviewed and updated. If it is out of date or no longer required, it should be deleted or disposed of confidentially.

- Telemedicine Clinic has provided training to all employees (and will provide training to new employees) to help them understand their responsibilities when handling personal data.

  SOP-IT-013 TMC IT Users Groups and permission Administration
  SOP-TMC-055 TMC Protecting PII SOP
  POL-TMC-005 TMC Password Policy

8.18 Privacy by default and privacy by design

- Each new process or technical asset needs to be evaluated based on data protection risks and consider data minimisation. This should be documented, and a Privacy Impact Assessment (PIA) should be produced if so required. This is described in SOP-TMC-039 Unilabs_Data Protection Impact Assessment Guidance and SOP-TMC-035 Data Privacy Impact Assessment

- Security measures should be implemented to minimise risks for the data subjects => Privacy by design

- Ensuring by default that only personal data*, which is necessary for each specific purpose, is processed. Relevant factors are: the amount of data collected, the extent of their processing, the period of their storage and their accessibility => Privacy by Default

- These processes are described in SOP-TMC-033 Data Protection by Design and by Default and SOP-TMC-041 Unilabs_Guidance on Privacy by Design by Default

8.19 Data transfer to third countries

- According to the data protection regulation, to ensure the protection of the personal data, TMC must put in place relevant safeguards such as Data Processing Agreements based on the Standard Contractual Clauses issued by the European Commission, and technical security measures.

- The Data Processing Agreements are stored on Finance intranet.

- DOC-TMC-046 Guidelines on International Data Transfers between TMC entities and clients describes what we transfer and how we transfer personal data.

- The specific safeguards for each transfer are documented in DPIAs and in the Data Processing Inventory.

8.20 Information Security and Privacy events and weaknesses, data breaches

- All Information Security and/or Privacy events, suspected weaknesses and data protection breaches are to be reported to the Security officers (through Security Incident - All Items) and in case of possible implications for patients also to the Medical Director. All Information Security and/or Privacy events shall be investigated to establish their cause and impacts with a view to avoiding similar events.

- The data controllers, if other than TMC, should be informed, if any data breaches or incidents create a risk for their data subjects.

- TMC, in the role of Data Controller, must report data breaches to the relevant data protection authorities within 72 hours if the breach is likely to result in risk to the rights and freedom of natural person in case of high risk for the data subjects. Moreover, TMC should ensure the data subjects are informed in case of data breaches that create a risk for them.

- If a data breach is determined as “high” or “critical”, it needs to be reported to the TMC Board and the Data Protection Officer.

- TMC, in the role of Data Processor, should ensure the clients are informed in case of data breaches related to their data.

- This is documented in SOP-TMC-034 Data Protection Breaches process

- The process includes how to register the incidents, how to review them and the way to communicate them to data subjects, data controllers and others.

- TMC may face significant fines for a data breach or for failing to adhere to the General Data Protection Regulations.

- Employees should be aware they can be criminally liable if they knowingly or recklessly disclose personal data. Serious breaches of this Policy may be treated as a disciplinary offence.
  SOP-TMC-034 Data Protection Breaches process
  SOP-TMC-038 Unilabs - Global Data Breach Notification procedure

8.21 Classification of Sensitive Information.

- A consistent system for the classification of information enables common assurances in information partnerships, consistency in handling and retention practice when information is shared with other bodies.

- TMC shall implement appropriate information classification controls, based upon the results of formal risk assessment.

- The classification is described in POL-TMC-007 TMC Documentation Convention Policy and guidelines and SOP-TMC-052 Unilabs Group Information Classification and Handling Procedure

8.22 Reporting

- The TMC Security and Quality Board shall keep the CEO and the SLT informed of the Information Security and Privacy status of the organisation by means of regular reports and presentations.
  SOP-TMC-006 Data analysis

8.23 Data on paper

- Where data is stored on paper, it should be safely stored in a secure place where unauthorised personnel cannot see it. In particular; -
  - When not required, files or other paper based personal data should be kept in a locked drawer or filing cabinet.
  - Employees should make sure papers are not left where unauthorised people could see them (e.g. on a printer).
  - Documents should be confidentially shredded and disposed of securely when no longer required.

- These responsibilities also apply to data that is usually stored electronically but has been printed out for some reason.

8.24 Security Control of Assets

- Each IT asset (hardware, software, application or data) is inventoried and under control of the IT department.
  SOP-IT-010 Maintenance and End of Life Tasks for TMC Workstations, Laptops, Servers and Network Devices

8.25 Access Controls

- Only authorised personnel who have a justified and approved business need shall be given access to restricted areas containing information systems or stored data.

  Physical access: POL-TMC-001 TMC Access Policy
  Computer access: POL-IT-002 Network Security Policy

8.26 User Access Controls

- Access to information shall be restricted to authorised users who have a bona-fide business need to access the information.
- Data should be protected by strong passwords that are changed regularly.

  Physical access: POL-TMC-001 TMC Access Policy
  Computer access: POL-IT-002 Network Security Policy

8.27 Computer Access Control

- Access to computer facilities shall be restricted to authorised users who have business need to use the facilities.

  Physical access: POL-TMC-001 TMC Access Policy
  Computer access: POL-IT-002 Network Security Policy

8.28 Application Access Control

- Access to data, system utilities and program source libraries shall be controlled and restricted to those authorised users who have a legitimate business need e.g. systems or database administrators. Authorisation to use an application shall depend on the availability of a licence from the supplier.
  POL-TMC-035 Unilabs Group User Access Management Procedure

8.29 Equipment Security

- To minimise loss of or damage to all assets, equipment shall be physically protected from threats and environmental hazards.
- Data should only be stored on designated drives and servers.
- Servers containing personal data should be sited in a secure location, away from the general office and Data should be backed up frequently.
  SOP-ISMS-001 Statement of Applicability 27001-2013

8.30 Computer and Network Procedures

- Management of computers and networks shall be controlled through standard documented procedures that have been authorised by the TMC Security and Quality Board.

8.31 Protection from Malicious Software & Cybersecurity

- The organisation shall use software countermeasures and management procedures to protect itself against the treat of malicious software.

- All staff shall be expected to co-operate fully with this policy and must read, sign and comply with the corresponding Unilabs Group Charter: POL-TMC-031 Unilabs Group Cybersecurity Charter.

8.32 User media

- The use of all removable media including USB Flash and USB hard disks is not permitted. Exclusions to this are only permitted with a valid and justifiable business case. TMC uses Antivirus Software to control the use of removable media.
  POL-TMC-011 TMC Security and Confidentiality User guidelines

8.33 Monitoring System Access and Use

- An audit trail of system access and data use by staff shall be maintained and reviewed on a regular basis.

- TMC has in place routines to regularly audit compliance with this and other policies. In addition, it reserves the right to monitor activity where it suspects that there has been a breach of policy. The regulations permit monitoring and recording of employees' electronic communications for the following reasons:
  - Establishing the existence of facts
  - Investigating or detecting unauthorised use of the system
  - Preventing or detecting crime
  - Ascertaining or demonstrating standards which are achieved or ought to be achieved by persons using the system (quality control and training)
  - In the interests of national security
  - Ascertaining compliance with regulatory or self-regulatory practices or procedures
  - Ensuring the effective operation of the system.

  User Admin and Accounts Lifecycle Policy

8.34 Accreditation of Information Systems

- The organisation shall ensure that all new information systems, applications and networks meet the security requirements defined and approved by the TMC Security and Quality Board before they commence operation.
  Security assessment V2 - PROJECT NAME - DATE (1)

8.35 System Change Control

- Changes to information systems, applications or networks shall be reviewed and approved by the Head of IT, member of the TMC Security and Quality Board and revised in the Steering Committee.
  SOP-IT-031 IT Change Management Procedure

8.36 Intellectual Property Rights

- The organisation shall ensure that all information products are properly licensed and approved by the Head of IT. Users shall not install software on the organisation's property without permission from the IT manager. Users breaching this requirement may be subject to disciplinary action.

POL-TMC-011 TMC Security and Confidentiality User guidelines

8.37 Business Continuity and Disaster Recovery Plans

- The organisation shall ensure that business impact assessment, business continuity and disaster recovery plans are produced for all mission critical information, applications, systems and networks.
- TMC has implemented a Business Continuity strategy that includes the governance and overview of the Business Continuity work in the company
  POL-TMC-039 Business Continuity Strategy
  SOP-TMC-015 TMC Contingency Plans management

9. Further Information

Further information and advice on this policy can be obtained from TMC Local Data Protection Coordinators (dataprotection@telemedicineclinic.com).

All undersigned assume and fully accept the contents of this Policy and agree to implement it within their respective areas to ensure the proper Management of the Information Security System and the Privacy Information Management System.

Head of Operations and
Head of Quality and Regulatory Affairs
Ida Anderman

DocuSigned by:
Ida Anderman
FDB7F111B76C495...

28-May-2024 | 14:29 CEST

ISMS Manager
Javier Castillo

DocuSigned by:
Javier Castillo
0F178C820BF84B8...

28-May-2024 | 14:20 CEST