Privacy Policy for mediduxTM
Web application for healthcare professionals

Contents

1. Roles and responsibility 2
2. Provider and data protection contact 2
3. Scope 2
4. Data processed 3
4.1 User data of healthcare professionals 3
4.2 Usage, interaction and system data 3
4.3 Patient data accessed within the institution 3
5. Purposes of data processing 4
6. Legal bases 4
7. Authentication and security 4
8. Recipients, partners and service providers 4
9. Interfaces, HIS/PIS and interoperability 5
10. Reviews, additional services and service processes 6
11. Product improvement, analytics and quality assurance 6
12. Service providers and processors 6
13. Retention period 7
14. Rights of data subjects 7
14. Amendments 7

1. Roles and responsibility

This Privacy Policy explains how personal data are processed when physicians, other healthcare professionals and authorised administrative users use the medidux™ web application.

Where healthcare professionals access or process patient data through the web application in the course of their work, this generally takes place under the responsibility of the relevant institution, in particular the hospital, practice or organisation responsible for that data processing under data protection law.

mobile Health AG provides the web application as a technical platform and processes data in its capacity as provider and service provider in accordance with applicable contractual and legal requirements.

Processing is carried out in compliance with applicable legal requirements, in particular the Swiss Federal Act on Data Protection (FADP) and, where applicable, the European Union General Data Protection Regulation (GDPR). Terms such as “personal data”, “health data” and “processing” are defined in particular in Article 5 FADP and Article 4 GDPR.

2. Provider and data protection contact

mobile Health AG
Mühlebachstrasse 43
8008 Zurich
Switzerland
Email: contact@mobilehealth.ch
Telephone: +41 43 243 76 22

Data protection contact:
datenschutz@medidux.com

3. Scope

This Privacy Policy applies to use of the medidux™ web application by:

- physicians,
- healthcare professionals,
- authorised administrators,
- and, where applicable, other authorised user roles in an institutional context.

4. Data processed

4.1 User data of healthcare professionals

When the web application is used, the following data may in particular be processed:

- name,
- business email address,
- function / role,
- institution,
- login data,
- authorisation status,
- HIN-related authentication information, where used.

4.2 Usage, interaction and system data

The following may also be processed in particular:

- login times,
- access events,
- functions used,
- processing steps,
- technical log data,
- security and error data,
- data concerning permissions and role changes.

4.3 Patient data accessed within the institution

Where you access patient data through the web application as an authorised healthcare professional, health-related data are also processed as part of platform use, in particular:

- symptoms,
- wellbeing,
- vital signs,
- medication,
- notes,
- progress data,
- alerts,
- laboratory and IVD-related data, including entered or transmitted test results such as blood glucose and CRP values,
- medical events and event records, including information about consultations, emergencies, hospitalisations, treatments or other care-related events,
- genomics, molecular pathology and biomarker data, where provided for in the relevant care context,
- form, registry and study data, where medidux™ is used for these purposes,
- data relating to interdisciplinary medical meetings, specialist consultations and boards, including case summaries, questions, recommendations, decisions, minutes and associated medical information,
- other health-related entries recorded or displayed through the intended functions.

5. Purposes of data processing

Data are processed in particular for the following purposes:

- providing and securely operating the web application,
- managing user accounts, roles and permissions,
- authentication and access control,
- providing patient-related overviews and functions,
- processing alerts, reviews and documentation functions,
- supporting interdisciplinary medical meetings, specialist consultations and boards where medidux™ is used for this purpose,
- recording, displaying or transmitting form, registry, study, biomarker, genomics or molecular pathology data where included in the relevant service scope,
- connecting to third-party systems, such as HIS, practice information systems or laboratory systems, where provided,
- conducting and supporting study processes where medidux™ is used for clinical or other studies,
- support, maintenance and further development of the web application,
- error analysis, quality assurance and system security.

6. Legal bases

Where required by applicable law, personal data are processed in particular on the basis of Articles 6 and 30 et seq. FADP and, where applicable, Article 6(1)(b) and (f) GDPR.

7. Authentication and security

Access is provided through personalised user accounts. In the Swiss version, authentication procedures through the HIN network may be supported in particular to enhance access security.

Technical and organisational security measures may be used to ensure security, availability and traceability, including:

- access controls,
- logging,
- permission management,
- audit logs,
- security and error monitoring.

8. Recipients, partners and service providers

We disclose personal data only where legally permitted and, in particular, where necessary to provide platform functions, medical care, organisational administration or technical delivery of the services.

Recipients or categories of recipients may include in particular:

- treating institutions and healthcare partners, in particular hospitals, clinics, practices or other healthcare providers whose users or patients are managed, connected or cared for through the web application,
- authorised healthcare professionals, care teams, study centres, study physicians and staff, registry offices or other authorised bodies in the relevant treatment, care, registry or study context,

- medical or telemedicine service providers supporting care, monitoring, triage, reviews, contact or support processes on behalf of or in cooperation with treating institutions or with us,
- hosting and cloud service providers,
- email service providers,
- SMS or communications service providers,
- support, monitoring, analytics and security service providers,
- laboratory and diagnostic systems and laboratory management systems,
- genomics, molecular pathology and biomarker systems where provided for in the relevant context,
- practice information systems (PIS), hospital information systems (HIS) and other interface or integration partners,
- providers or systems supporting interdisciplinary medical meetings, specialist consultations and boards where provided for in the relevant context,
- registry offices, registry platforms or registry-related service providers where medidux™ is used in a registry context,
- study platforms, study centres, study physicians and staff or other study-related service providers where medidux™ is used in a study context,
- product improvement, quality assurance, monitoring, analytics or security tools,
- administrative or billing service providers,
- other recipients, partners or service providers where provided for in the relevant context, necessary for the agreed service and legally permitted.

Personal data are disclosed to recipients or service providers only as permitted by law, in particular on the basis of statutory authorisation, contractual necessity, consent or overriding legitimate interests. Where third parties are engaged as processors, they are selected with due care, contractually required to comply with applicable data protection requirements, and instructed and monitored in accordance with applicable law.

9. Interfaces, HIS/PIS and interoperability

The web application may be connected to third-party systems through technical interfaces, in particular APIs, such as:

- practice information systems (PIS),
- hospital information systems (HIS),
- laboratory management systems,
- other medical or administrative systems.

Interoperability may use established standards, in particular HL7, FHIR or comparable formats. Responsibility for proper connection, system configuration and compliance with data protection requirements relating to third-party systems generally rests with the connecting institution or the contractual partners involved.

10. Reviews, additional services and service processes

Where additional services are offered in connection with the web application, such as structured reviews, professional analyses or other support services, the necessary data may be processed to the extent required. Such services may be subject to separate terms, contracts or billing arrangements.

Where medidux™ is used for clinical or other studies, it may also support study-related processing of data, roles, permissions, documentation and communications to the extent required. Such processing is carried out in accordance with applicable legal, organisational and study-specific requirements.

11. Product improvement, analytics and quality assurance

The Provider may process usage, interaction and system data to ensure operation, analyse errors, assure quality, and further develop and improve the web application.
Where data are anonymised or can be analysed without identifying individuals, they may be used in particular for:

- statistical analyses,
- product improvements,
- security analyses,
- optimising functions,
- optimising usage processes,
- technical and organisational quality assurance

and related purposes.

Pseudonymised data are processed only where legally permitted and in compliance with applicable data protection requirements.

12. Service providers and processors

External service providers may be engaged to provide and operate the web application, in particular for:

- hosting / cloud services,
- email and communications services,
- SMS services,
- support and maintenance,
- monitoring, analytics, quality assurance and security services,
- integration and interface services,
- laboratory, diagnostic, genomics, molecular pathology, PIS, HIS or other interface and integration systems where provided for in the relevant context,
- services or systems supporting interdisciplinary medical meetings, specialist consultations and boards where provided for in the relevant context,
- registry, study or documentation platforms where medidux™ is used in the relevant context,
- administrative or billing services where provided for in the relevant context.

Personal data are transferred to such service providers only where legally permitted and subject to appropriate contractual safeguards.

13. Retention period

Personal data are processed and stored only for as long as necessary for the stated purposes. They may be retained longer only where required by statutory, regulatory, contractual or documentation obligations, or where necessary to establish, exercise or defend legal claims.

14. Rights of data subjects

Where the statutory requirements are met, you have in particular the following rights:

- the right of access under Article 25 FADP or Article 15 GDPR;
- the right to rectification under Article 32 FADP or Article 16 GDPR;
- the right to erasure under Article 32 FADP or Article 17 GDPR;
- the right to restriction of processing under Article 32 FADP or Article 18 GDPR;
- the right to data disclosure or portability under Article 28 FADP or Article 20 GDPR;
- the right to withdraw consent, where applicable;
- the right to lodge a complaint with a competent supervisory authority.

Data subjects also have the right to lodge a complaint with a competent data protection authority. The authority generally responsible at the Provider's registered office is the Swiss Federal Data Protection and Information Commissioner (FDPIC). Where the GDPR applies, a complaint may also be lodged with the competent European supervisory authority.

14. Amendments

This Privacy Policy may be amended as needed, in particular due to legal, regulatory, technical or operational changes.