Data Processing Regulations

Table of Contents

1. Initial position

CONCORDIA Swiss Health and Accident Insurance Ltd is the controller of the automated data collection pursuant to the Swiss federal law on health insurance (KVG/LAMal). The purpose of the data collection is to process and implement health and accident insurance within the realm of mandatory health care insurance in accordance with the KVG/LAMal.

The Data Processing Regulations also apply, in accordance with Art. 59a of the Health Insurance Ordinance (KVV/OAMal), to the independent data connection point, which is operated internally by CONCORDIA.

2. Documentation of the organisational units affected by the system

CONCORDIA Swiss Health and Accident Insurance Ltd is the system operator and, as the controller of the automated data collection, the body that is responsible for it.

3. Interface Description

3.1 Interfaces to external data users or data providers

Pursuant to Art. 84 of the KVG/LAMal, several services, which also partially includes the processing of personal data, have been outsourced by CONCORDIA to external partners for document processing and postal solutions. The data-compliant processing of data, as well as data security, has been regulated in the respective cooperation agreements. Furthermore, the IT partners are partially certified in accordance with various ISO norms, such as the ISO 9001:2008 (quality management systems) and the ISO/IEC 27001 (information security management systems) in particular.

Furthermore, as the controller of the data collection, CONCORDIA remains responsible for the compliance with data protection for the outsourced areas (Art. 22 of the Ordinance to the Federal Act on Data Protection VDSG/OLPD/OFADP).

As part of the implementation and processing of health and accident insurance in the realm of mandatory health care insurance in accordance with the KVG/LAMal, CONCORDIA maintains interfaces to data users and data providers, which are described hereinafter.

Recipient / Supplier	**Object**	**Particularly sensitive data**	**Trigger**
Banks	Monetary transactions	No	Automatic
Public authorities / Courts	Art. 82 KVG/LAMal, Art. 84a KVG/LAMal	Yes	Manual
External printing companies	Customer magazine	No	Automatic
Financial service providers	Bank master	No	Automatic
Joint institutions under the KVG/LAMal	Risk allocation, hospital days	No	Manual
HMO partner	Art. 84a KVG/LAMal	Yes	Manual
Internet comparison services	Calculated offers	No	Automatic
Cantons	Individual premium reduction (IPV/RIP/IPR), Art. 64 KVG/LAMal	Yes	Automatic
Service provider	Art. 84a KVG/LAMal, Art. 59 KVV/OAMal	Yes	Automatic / manual

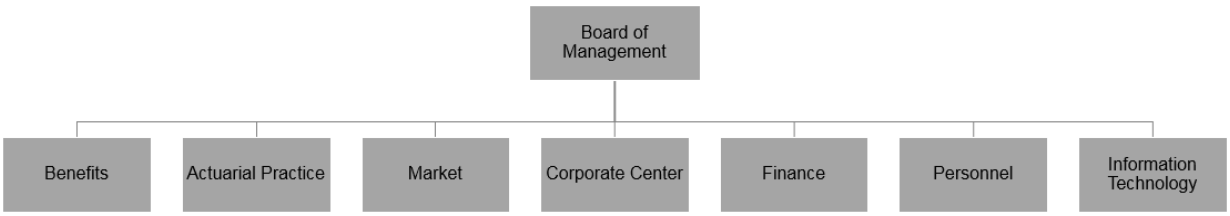
Recipient / Supplier	Object	Particularly sensitive data	Trigger
Medidata	Exchange platform of electronic documents	Yes	Automatic
Tele-medical service partners	Health care	Yes	Manual
santésuisse	Information, Register of paying agents (ZSR/RCC), Data pool	No	Automatic
Sedex	Individual premium reduction (IPV/RIP/IPR)	Yes	Automatic
Social insurance provider	Art. 84a KVG/LAMal	Yes	Manual
SwissPost Solutions	Notification of payment receipts	No	Manual
Insurance card (VeKa/Cada/Teda)	Insurance card (Art. 42a KVG/LAMal, Ordinance on the insurance card for obligatory health care insurance (VVK/OCA/OTeA))	Yes	Automatic
Insured persons	Information, correspondence, accounting of benefits	Yes	Automatic / manual
Central contract registry (ZVR/RCCo)	Information	No	Manual

3.2 Data source

The data are provided by service providers, insured persons, other social insurance providers, public authorities and financial services providers.

4. Organisation chart of the data collecting body

Organisation chart of CONCORDIA Swiss Health and Accident Insurance Ltd



5. Responsibilities

As the controller of the data collection, the Board of Management of CONCORDIA Swiss Health and Accident Insurance Ltd is responsible for complying with data protection rules and data security.

Representatives for data protection, information security and physical security are there for matters regarding data protection and data security. These representatives advise the Board of Management, establish guidelines and are also involved in the control processes.

6. Documentation on the planning, implementation and operation of the data collection

The operation of the data collection is recorded in specific operation manuals. The technical planning and implementation is documented in project documents. The technical documentation of systems components can be found in computer science operation manuals.

7. Registering the data collection with the Federal Data Protection and Information Commissioner (EDÖB/PFPDT/IFPDT/FDPIC) after consulting with the data protection officer

In accordance with Art. 11a, para.5, let. E of the Swiss Federal Act on Data Protection (DSG/LPD/FADP), CONCORDIA Swiss Health and Accident Insurance Ltd has designated an independent data protection advisor who independently monitors internal compliance with data protection regulations and maintains a register of the data collection. For this reason, CONCORDIA is exempt from the obligation to notify the EDÖB/PFPDT/IFPDT/FDPIC of the data collection as per Art. 11a, para. 2 of the DSG/LPD/FADP.

CONCORDIA fulfils the requirement to submit process documentation to the EDÖB/PFPDT/ IFPDT/FDPIC pursuant to Art. 84b of the KVG/LAMal.

8. Process documentation pertaining to the data collection

The data processing procedures for the data collection processes are recorded in internal process documentation.

9. Data source

See table, chapter 3

10. Purposes for which data is regularly disclosed

See table, chapter 3

11. Control procedures and in particular the technical and organisational measures as per Art. 20 of the Ordinance to the Swiss Federal Act on Data Protection (VDSG/OLPD/OFADP)

Adequate technical and organisational measures have been implemented, which ensure the confidentiality, integrity and availability of the data.

11.1 Entrance control

To ensure that no unauthorised persons access the commercial property of CONCORDIA, entry is possible only to the employees of CONCORDIA who possess a badge or key.

Access to the commercial property of CONCORDIA is regulated in the guidelines entitled “Zutritt zu Betriebsliegenschaften der CONCORDIA” (entering the commercial property of CONCORDIA) and “Zutritts- und Schliessorganisation” (entrance and closure organisation).

There is an additional directive entitled “Zutrittsrechte bei der Informatik” (rights of entry to information technology) regarding entry to the computing premises.

11.2 Data media control

By means of technical and organisational measures, CONCORDIA ensures that no unauthorised persons may read, copy, modify or delete data; that no unauthorised data is stored in the memory; and that no unauthorised personal data is inspected, modified, deleted or stored.

Certain modifications conducted by employees may be traced back in the system.

Employees are instructed in various directives and regulations on the proper handling of data. One crucial directive is entitled “Umgang mit Hardware, Software und elektronischen Daten” (dealing with hardware, software and electronic data).

Digital data media is disposed of by the information processing business unit by means of a regulated process.

11.3 Transport control

By means of technical and organizational measures, CONCORDIA ensures (e.g. with encryption or directives on e-mail handling) that no unauthorised persons may read, copy, modify or delete data when disclosing personal data or when transporting data media.

11.4 Disclosure control

The recipient of personal data is verified either manually or by means of technical devices.

11.5 Storage control

See 11.2

11.6 User control

CONCORDIA has at its disposal an appropriate multilevel security concept according to the level of data protection required. Users must be authenticated in order to gain access to the information systems.

11.7 Access control

Authorisation for access to data is assigned on a strictly need-to-know basis – that is, rights will only be assigned in order to exercise the function required. Assignment is based on authorisation profiles. Defined work processes are in place for user and authorisation management, and these are supported by technical devices.

The assigned authorisations are verified periodically as part of the internal control processes.

11.8 Input control (log file)

The personal data entry is stored chronologically in the central information system. In the event of abuse or the suspicion of abuse, this data may be analysed. Employees are informed accordingly in the regulations entitled “Umgang mit Hardware, Software und elektronischen Daten” (dealing with hardware, software and electronic data).

12. Description of data fields and organisational units with access to them

As part of the reporting processes for the data collection, the data fields are described and the authorisation concept is documented in separate processing regulations.

13. Type and extent of user access to the data collection

Each employee only has access to that data which he needs to fulfil his tasks.

How access takes place, which authorisation profiles (roles) can exercise which functions, and which data space may be accessed are stipulated in an authorisation concept, where likewise, who is allowed to apply for these roles and who must grant the assignment are defined and approved.

The employees of CONCORDIA have no access to minimal clinical data (MCD) set that is received and processed automatically by the independent data connection point. Should invoices be selected by the independent data connection point for verification, the employees assigned with verifying the case receive access to the invoices as well as the MCD associated with it until the case is closed.

14. Data processing procedures, in particular the procedures for rectifying, blocking, anonymising (pseudonymising), storing, safeguarding, archiving or destroying data

The data processing procedures are documented in specific directives, regulations and manuals (see also chapters 13 - 15).

Users of a data collection are regularly trained on matters concerning specialist processes and data protection.

15. Configuration of information technology resources

The information technology resources deployed by CONCORDIA (hardware and software) meet standards that are both international as well as those that are customary in the sector. The information technology resources are subject to a regulated life cycle management process.

The configuration of information technology resources is documented in operating manuals and is updated as required.

16. Procedure for exercising the right to information

In accordance with Art. 8 of the DSG/LPD/FADP, requests for information should be directed to the company data protection officer at:

CONCORDIA Swiss Health and Accident Insurance Ltd
Data Protection Officer
Bundesplatz 15
6002 Lucerne