

Processing regulations SwissDRG

Valid from 01.02.2017

Table of contents

Section 1: General provisions	3
1.1. Legal basis	3
1.2. Objective of processing regulations	3
1.3. Purpose of data processing	3
1.4. Responsible unit	3
1.5. Duty of confidentiality pursuant to Art. 33 of the Federal Act on the General Part of Social Insurance Law (ATSG)	3
Section 2: Structure of SwissDRG data processing	4
2.1. Structure of information systems used for SwissDRG processing	4
2.2. Interfaces	5
Section 3: Units involved	5
3.1. Regional customer services	5
3.2. Central organisational units	5
3.3. Application owners	5
3.4. VAD	5
3.5. Coding experts / SwissDRG specialists	5
Section 4: Users and data access	6
4.1. Users	6
4.2. User management	6
4.5. DAS access and access authorisation	6
4.6. VAD access and access authorisation	6
Section 5: Processing of data / data categories	7
5.1. Data collection	7
5.2. Data categories for health insurance contract	7
5.3. Data processing pursuant to Art. 42 KVG and disclosure of data pursuant to Art. 84a KVG	7
5.4. Data processing on behalf of Helsana Group companies	7
Section 6: Storage period, deletion of data	8
6.1. Archiving obligation, storage and deletion of data	8
6.2. Storage of diagnosis-related data pursuant to Art. 59a ^{ter} of the Health Insurance Ordinance (KVV)	8
Section 7: Technical and organisational measures	8

7.1	Access control.....	8
7.2	Control of personal data carriers	8
7.3	User authentication	9
7.4	Disclosure control	9
7.5	Protocols	9
7.6	User support and notification requirements	9
7.7	Supervision and responsibility	9
Section 8: Rights of affected parties		10
8.1	Obligation to provide information pursuant to Art. 18a DSG	10
8.2	Rights of insured persons under Art. 42 para. 5 KVG	10
8.3	Right to receive information	10
8.4	Rights to update and delete data	10
Section 9: Final provisions.....		10
9.1	Enclosures	10
9.2	Amendments to the regulations	10
9.3	Entry into force	11
ENCLOSURE 1		12
ENCLOSURE 2		13
ENCLOSURE 3		14
ENCLOSURE 4		16
ENCLOSURE 5		17
ENCLOSURE 6		18

Section 1: General provisions

1.1. Legal basis

Based on Art. 21 of the Ordinance to the Federal Act on Data Protection (VDSG) in conjunction with Art. 84 of the Federal Health Insurance Act (KVG) and Art. 49 KVG, Helsana Insurance Company Ltd (Helsana) adopted the following processing regulations for the automated processing of sensitive data and personality profiles relating to the SwissDRG rate agreements.

1.2 Objective of processing regulations

These processing regulations in particular describe the data processing and control procedures and electronic data processing operations. It contains information about the body that is responsible for data protection and data security, the origin of the data and the purposes for which the data are regularly disclosed, and describes the process for authorising access to the modules of the electronic information system.

1.3 Purpose of data processing

The purpose for which data are gathered is governed by the Federal Health Insurance Act (KVG). Health insurance companies are responsible for the management of the health insurance in accordance with the KVG.

Under Art. 84 KVG, the bodies entrusted with the management, monitoring or supervision of the implementation of the KVG are authorised to process the personal data, including sensitive data and personality profiles, which they need in order to carry out the tasks delegated to them by the law.

Under Art. 49 KVG, inpatient treatment is charged at diagnosis-related case-based flat fees (Swiss-DRG, diagnosis-related reimbursement groups). The insurance company must be provided with information on the principal and secondary diagnoses as well as the treatment and procedures. This information is included in the minimal clinical dataset (MCD).

According to Art. 32 KVG, benefits must be effective, expedient and cost-effective. Under Art. 56 KVG, health insurance companies are obliged to check that benefits are cost-effective.

1.4 Responsible unit

Helsana is responsible for the management of the health insurance and is therefore the recipient of invoices for inpatient benefits that qualify as diagnosis-related reimbursement groups (SwissDRG). Helsana is also the owner of the database or the Helsana information system in which the data are processed and captured.

With the measures defined herein, Helsana ensures compliance with the provisions.

1.5 Duty of confidentiality pursuant to Art. 33 of the Federal Act on the General Part of Social Insurance Law (ATSG)

All employees are obligated to uphold the duty of confidentiality pursuant to Art. 33 ATSG. If they violate this duty of confidentiality, they are subject to the specific penal provisions of Art. 54 of the Health Insurance Oversight Act (KVAG). Employees are aware of the sanctions.

In conjunction with their employment contract, employees are obligated to maintain secrecy and confidentiality.

Section 2: Structure of SwissDRG data processing

2.1 Structure of information systems used for SwissDRG processing

The SwissDRG data are sent by the service providers either to Administration or on request of the insured person or in justified cases to the medical examination service (VAD). The data are captured in the database of the Helsana information system (management of health insurance). This is a modular system. The following sub-systems and contents are involved in the processing of payments for inpatient treatment:

Health Insurance Administration Information System

1. Sub-system for contract data (surname, first name, date of birth, gender, insurance number, address, etc.)
2. Sub-system for insurance cards (data pursuant to Art. 49a KVG, i.e. surname, address, AHVN13, insurance number of insured person, insurance coverage, suspensions)
3. Sub-system for benefit processing (benefit data, processing pursuant to Art. 42 KVG)
4. Sub-system for medical information (service provider invoices and other customer documents, including medical information relating to invoices provided by service providers pursuant to Art. 42 KVG).
5. Sub-system for archived documents/medical information
6. Sub-system for medical examination services VAD (data pursuant to Art. 49a KVG, i.e. name, address, insurance number of the insured person, insurance coverage, suspensions, benefit data, processing pursuant to Art. 42 KVG or service provider invoices and other customer documents, including medical information relating to invoices provided by service providers pursuant to Art. 42 KVG)
7. Sub-system for customer contact: Correspondence with insured persons (name, insurance number, medical information)
8. Sub-system for management of inpatient claims
9. Sub-system for the special management and benefit processing of complex cases:

VAD information system:

1. Service provider invoices and other customer documents, including medical information relating to invoices provided by service providers pursuant to Art. 42 KVG
2. Sub-system: Helsana employee insurance

2.2 Interfaces

Various interfaces enable direct contact with service providers, for example, service providers settle directly with Helsana. The data flow diagram is shown in enclosure 3.

The SwissDRG invoices are sent to Helsana by the service provider as an XML invoice. Data are transmitted in encrypted form.

Service providers who are not yet electronically linked send their invoices and MCD via regular mail to Helsana's data collection point (see enclosure 4).

The data are sorted according to the reference used by the service provider. If mail is marked VAD, it is sent to the VAD and if not, the MCD is sent to Administration.

Section 3: Units involved

3.1 Regional customer services

Payments for inpatient invoices pursuant to the KVG are processed by regional customer service employees. For this task they process benefit and personal data including sensitive personal data in Helsana's information system or the specific sub-systems in accordance with section 2.1.

Payment is made by the competent regional customer service unit.

3.2 Central organisational units

Employees and auxiliaries in the following areas have access to Helsana's information system and its sub-systems in order to process inpatient invoices pursuant to the KVG:

1. Benefits management
2. Central medical examination service (VAD)

3.3 Application owners

The application owners of Helsana's information system and sub-systems are responsible for compliance with the provisions of the directives and regulations on data processing.

They are responsible for ensuring their application data are made available within the limits of the law only.

3.4 VAD

For cases under Art. 42 para. 5 KVG, the invoices are sent directly to the VAD and are processed by the medical examiners and VAD auxiliaries. They check the benefits under Art. 57 KVG and send their assessment to Administration so that the invoice can be approved for payment.

3.5 Coding experts / SwissDRG specialists

Employees responsible for coding (medical coders, coders, initial auditors) have full access to the medical data (diagnosis and procedures) in order to check the diagnosis and procedure codes.

Section 4: Users and data access

4.1 Users

Helsana employees have access to Helsana's information system if they need access to carry out their mandate to “manage the health insurance”.

Additional DRG access is given in particular to:

1. Data typists at the data collection point (DAS)
2. Initial auditors
3. Coders
4. Medical coders
5. Medical examiners and their auxiliaries
6. Helsana's system administrators

4.2 User management

There are documented processes for the management of users and their access rights (allocation, changes, deletion of authorised users) to Helsana's information system. The authorisation procedure is processed via the authorisation portal, which forwards the request for authorisation for review and approval to the competent application owner or the person who has to grant approval.

A VAD employee is responsible for managing authorisations to access the data of the medical examiner.

4.3 Training for users

Users attend internal courses where they are trained to use the different applications and sub-systems.

4.4 User manuals and processing guidelines

There are internal documents about the sub-systems. The sub-systems' user representatives manage the related documentation.

Data processing is also defined in directives, regulations and benefits manuals. These are regularly updated by the competent organisational units.

The specialist departments of the competent organisational units issue specific instructions to ensure that benefits under the KVG are assessed on the same level for the entire Swiss insurance region.

4.5 DAS access and access authorisation

An organisational solution has been introduced to regulate access for DAS employees to the locked DAS rooms. The DAS is located in one central place.

Access for DAS employees is based on a restrictive role model generated by function, membership and location.

4.6 VAD access and access authorisation

An organisational solution has been introduced to regulate access for DRG-VAD employees to the locked VAD rooms (access only by agreement with VAD). This means that VAD decides in agreement with the competent manager when and how long a DRG-VAD employee may work in the VAD rooms.

A report is drawn up that shows when DRG-VAD employees worked in the VAD rooms. These reports must be kept for 13 months. They are only accessible to the bodies or persons who are responsible for monitoring the data protection provisions and may only be used for this purpose.

Access for VAD employees is based on a restrictive role model generated by function, membership and location.

The job profile of a DRG-VAD employee makes it clear that VAD documents may only be processed in the VAD rooms.

Section 5: Processing of data / data categories

5.1 Data collection

The data are obtained from the providers of inpatient benefits pursuant to the KVG, during the processing of benefits and from the master data on the insured persons that are managed in the sub-systems.

5.2 Data categories for health insurance contract

Enclosure 1 lists the data categories that are needed to process SwissDRG invoices.

5.3 Data processing pursuant to Art. 42 KVG and disclosure of data pursuant to Art. 84a KVG

Data processing is done in compliance with Art. 42 KVG. Diagnosis data are processed only in order to check the invoices in compliance with the health insurer's obligation under Art. 56 KVG to ensure the cost-effectiveness of benefits.

Any further disclosure of data is exclusively governed by Art. 84a KVG. In a particular case and upon submission of a justified application, data may be forwarded in compliance with specific conditions, for example, to criminal courts and criminal investigation authorities, and with the written consent of the insured person, to third parties.

- Other possible recipients of data are listed in enclosure 2.

5.4 Data processing on behalf of Helsana Group companies

As part of the processing of inpatient SwissDRG invoices for the compulsory health insurance, Helsana processes personal data for its Group companies in application of Art. 84 KVG. Helsana also processes inpatient SwissDRG invoices for Helsana Accidents Ltd and for Helsana Supplementary Insurance Ltd.

Section 6: Storage period, deletion of data

6.1 Archiving obligation, storage and deletion of data

Documents that must be archived are stored for the period prescribed by law and protected against changes and unauthorised access. At the end of the statutory safekeeping period, the data must be deleted from Helsana's information system.

6.2 Storage of diagnosis-related data pursuant to Art. 59a^{ter} of the Health Insurance Ordinance (KVV)

Once the purpose for the processing has expired, only the VAD has access to the MCD sent to Helsana for the processing of payments.

When the processing is finished, the physical MCD are archived in a VAD room with access control.

The data are not additionally pseudonymised, but Administration's access is completely revoked.

At the end of the statutory safekeeping period, the the MCD must be deleted from Helsana's information system and the physical MCD destroyed.

Section 7: Technical and organisational measures

7.1 Access control

All rooms at Helsana are protected either electronically or manually from access by unauthorised persons. The Physical Security Officer keeps a log on the operation of all locking mechanisms.

The zones that need protection determine the security measures. Workplaces are protected from access by unauthorised third parties.

Rooms that need additional protection such as the VAD rooms, technical rooms, computer centres and the DAS room are protected as follows:

- The electronic data carriers in the computer centres operated by Helsana IT as well as the decentralised servers operated by Helsana IT have higher safety requirements and can only be accessed by specific authorised persons.
- The electronic data carriers in decentralised servers and computers that are not operated by Helsana's IT are subject to the same safety requirements as those operated by Helsana IT itself.
- The VAD and DAS rooms as well as the electronic sub-systems in which the diagnosis-related data are processed by authorised employees are completely separate from Administration. Only persons with an authorised badge have access to the VAD and DAS rooms.

7.2 Control of personal data carriers

IT safety measures are in place to ensure that only authorised persons can process the data on the electronic data carriers.

7.3 User authentication

Access to the sub-systems of Helsana's information system is protected by a user ID combined with an individual password that is valid for a limited time only.

The correct treatment of passwords is set out in an internal directive.

7.4 Disclosure control

The data recipients to whom personal data were disclosed by way of data transmission devices are identified by the interfaces, such as when service providers use the insurance card to check if there is coverage in accordance with Art. 49a KVG.

7.5 Protocols

In addition to the authorisation procedure, personal ID and password used to control access to Helsana's information system, some sub-systems produce automated processing protocols so that it is possible to subsequently determine whether the data were processed for the purpose for which they were gathered or disclosed. The protocols are prepared in application of Art. 10 VDSG and are kept for 13 months. They are only accessible to the bodies that are responsible for monitoring the data protection provisions and may only be used for this purpose.

7.6 User support and notification requirements

Users receive specialist support from the various specialist departments.

Technical support for data end devices, the network and applications is provided or arranged by Helsana's IT organisational unit.

Users are informed of the security level of Helsana's information system and are familiar with the rules for using the system and its data. These rules are explained in the operating manuals under "Information security". All users are obligated to report the following observations to the application owner or user representative:

- a. Errors in the captured data. Errors in the identity of the registered person (e.g. different information on the same person in the different sub-systems);
- b. Errors in the master data or their structures;
- c. Observed or suspected weaknesses or security defects in the system;
- d. Failure to implement or comply with security measures;
- e. Unforeseen events that could impact information security.

7.7 Supervision and responsibility

Sub-system application owners must ensure that users observe all directives as well as these processing regulations and enclosures.

Section 8: Rights of affected parties

8.1 Obligation to provide information pursuant to Art. 18a DSG

Under Art. 18a DSG, affected persons have to be informed when their personal data are collected. Given the statutory mandate under the KVG to process health data, the exceptions of Art. 18 para. 4(a) DSG apply, according to which the owner of the database no longer has an obligation to provide information if the law explicitly provides for the storage or disclosure of the data.

8.2 Rights of insured persons under Art. 42 para. 5 KVG

Insured persons may request that service providers only disclose their medical data to the medical examiner of the insurance company in accordance with Art. 57 KVG. This procedure is set out in enclosures 3 and 4.

8.3 Right to receive information

All individuals may ask Helsana whether their data are being processed. The right to receive information is governed by Art. 8 and 9 DSG as well as Art. 1 and 2 VDSG. Requests for information must be accompanied by a copy of an official identity document and sent to the address listed in enclosure 6.

The procedure is set out in an internal directive.

8.4 Rights to update and delete data

The rights of the persons affected to update and delete their data are governed by Art. 5 para. 2 and Art. 25 DSG (see enclosure 6).

Section 9: Final provisions

9.1 Enclosures

The following enclosures form an integral part of these processing regulations:

- Enclosure 1 Categories of processed personal data
- Enclosure 2 Categories of data recipients and participants
- Enclosure 3 Data flow diagram (electronic receipt) and explanations
- Enclosure 4 Data flow diagram (receipt by mail) and explanations
- Enclosure 5 Abbreviations
- Enclosure 6 Contact addresses

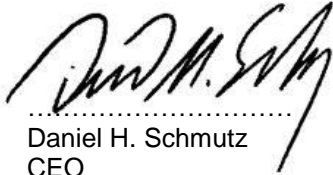
9.2 Amendments to the regulations

The processing regulations are regularly updated by the owner of the database as determined by Art. 11 VDSG. These regulations may be amended at any time. Amendments must be made in writing.

9.3 Entry into force

These regulations and enclosures replace the version of 1 December 2015 and enter into force on 1 February 2017.

Helsana Insurance Company Ltd



.....
Daniel H. Schmutz
CEO



.....
Robert Bächtiger
Head of Data Protection

Distribution list:

- Intranet
- www.helsana.ch

ENCLOSURE 1

Categories of processed personal data (Art. 3 para. 1(e) VDSG):

deutsch	französisch	italienisch
* Name, Vorname	Nom / Prénom	Nome / Cognome
* Geschlecht	Sexe	Sesso
* Geburtsdatum / Alter	Date de naissance / âge	Data di nascita / età
* AHVN13	Numéro AVS	Numero AVS
* Sprachen	Langues	Lingue
* Nationalität / Heimatort	Nationalité / lieu d'origine	Nazionalità / luogo di appartenenza
Kantons- / Gemeindezugehörigkeit	Appartenance cantonale / communale	Attinenza cantonale / comunale
* Versichertennummer	Numéro d'assuré	Numero d'assicurato
* Adresse	Adresse	Indirizzo
Bank- / Post-Verbindungen	Adresse bancaire / postale	Relazione bancaria / posta
Art der Versicherung und Deckung	Genre d'assurance et de couverture	Genere d'assicurazione e coperta
Art und Umfang der Leistungen	Genre et volume des prestations	Genere e entità delle prestazioni
* Gesundheitsdaten	Données sur la santé	Dati concernenti la salute
Leistungserbringer	Fournisseur de prestations	Fornitore di prestazioni
Eintritts- / Austrittsdatum	Date d'entrée / de sortie	Data entrata / uscita
Sistierung	Suspension	Sospensione
Versicherungsprämie	Prime d'assurance	Premio dell'assicurazione
Prämienfakturierung	Facturation des primes	Fatturazione dei premi
Franchisen	Franchise	Franchigia
Prämienverbilligungen Kanton	Réduction des primes par les cantons	Riduzione dei premi da parte dei cantoni
Inkassodaten	Données concernant les encaissements	Dati di incasso
Familie	Famille	Famiglia
Zivilstand	Etat civil	Stato civile
Versicherungen	Assurances	Assicurazioni
Zahlungen	Paielements	Pagamenti
Diagnosen	Diagnostics	Diagnosi
Arztberichte	Rapports médicaux	Rapporti medici
Telefonnummer	Numéro de téléphone	Numero die telefono
Daten Drittversicherer	Données assureurs tiers	Dati assicuratori terzi
Leistungskosten	Coûts de prestations	costi di prestazioni
* Hauptkategorie	Catégorie principale	Categoria principale

ENCLOSURE 2

Categories of data recipients (Art. 3 para. 1(f) VDSG):

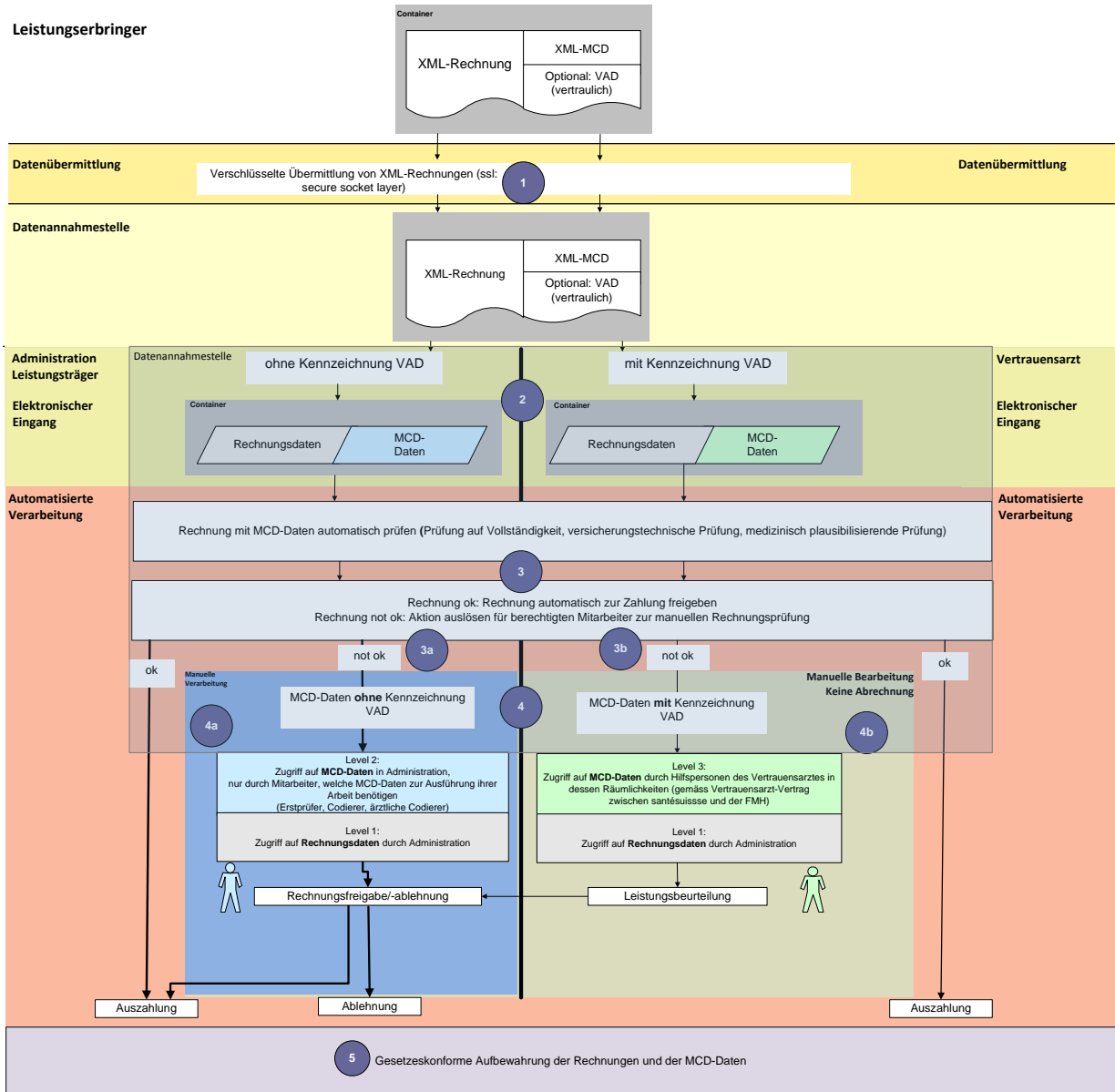
Versicherte	Assurés	Assicurati
Leistungserbringer	Fournisseurs de prestations	Fornitori di prestazioni
Behörden	Autorités	Autorità
Kanton	Canton	Cantone
Bundesorgane	Organes fédéraux	Organi federali
Versicherungen	Assurances	Assicurazioni
Soziale Institutionen	Institutions sociales	Istituzioni sociali
Leistungsempfänger	Bénéficiaires de prestations	Destinatari die prestazioni
Andere involvierte Kostenträger	Autres unités d'imputation impliquées	Altre unità di costo coinvolti
Rechtsdienst	Service juridique	Servizio giuridico
Vertrauensärzte	Médecins-conseilles	Medico di fiducia

Participant categories

Agenturen	Agences	Agenzie
Hauptsitz	Siège principal	Sede principale
Mitarbeiter	Collaborateurs	Collaboratori
Direktion	Direction	Direzione

ENCLOSURE 3

Data flow diagram (electronic receipt)



Automatische Triage der für den VAD bestimmten MCD ("VAD-Flag")
Kein Mitarbeiter hat Einsicht in die automatisierte Verarbeitung
In den Räumlichkeiten der Administration
Daten von der Administration einsehbar
Nur in den Räumlichkeiten des VAD
Nur Erstprüfer, Codierer und ärztliche Codierer haben Einsicht in die für die Verarbeitung benötigten MCD-Daten

Explanations to data flow diagram (electronic receipt)

1 Normally, the service provider transmits the invoice linked to the coded diagnosis and procedures (MCD) to Helsana's data collection point. In some cases, the service provider marks the diagnosis and procedures as confidential (in accordance with the standards of the data exchange forum). The data are transmitted in encrypted form via Medidata.

2 Helsana receives the electronic data and reads the data into the system (automated process). For decoupled transmission, the system links the invoice to the MCD or vice versa. This is done in accordance with the coupling fields defined by the data exchange forum.

3 The invoice processing system automatically checks the data for:

- Processability of dataset
- Completeness and validity (insurance rules)
- Indications of possible violations of statutory provisions, and
- Medical plausibility check (medical rules)

If none of these rules is tagged, the invoice is automatically approved for payment and the data are archived.

If a rule is tagged, an order to check the invoice is generated:

3a • if the diagnosis and procedures have not been flagged as confidential, the order is addressed to Administration

3b • if the diagnosis and procedures have been flagged as confidential by the service provider, the order is addressed to the medical examiner, i.e. only auxiliaries of the medical examiner have access to these diagnosis and procedure data

4 The invoices that were rejected by the system are checked manually:

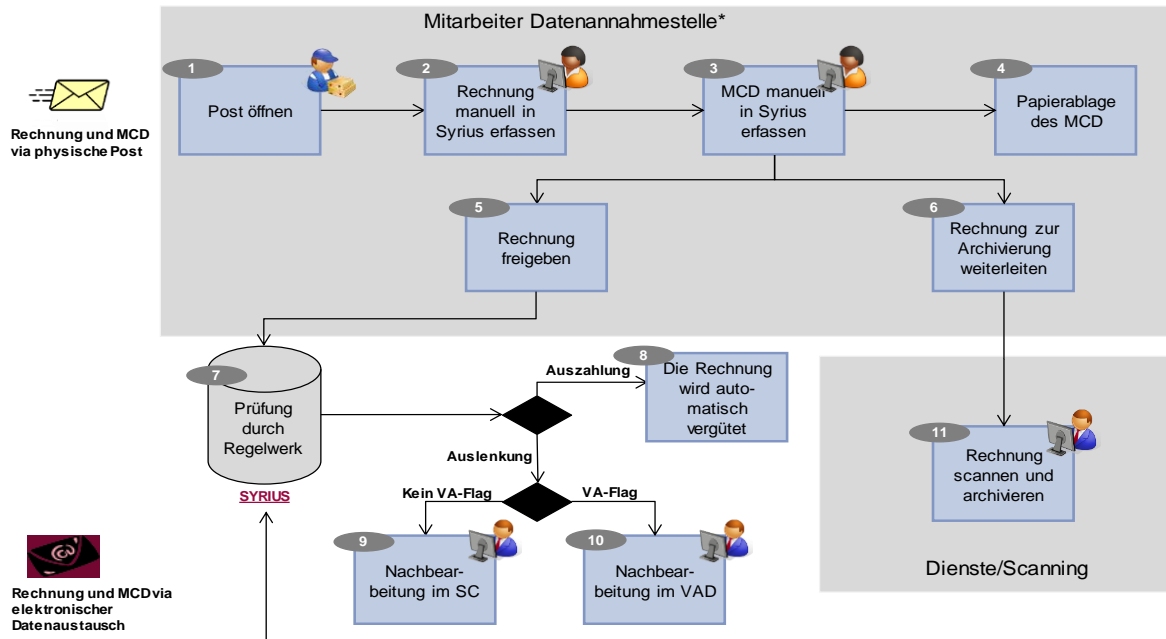
4a • if the diagnosis and procedures have not been flagged as confidential, the invoices are checked by Administration. Access to the diagnosis and procedure data is limited to the employees who need this data to do their work

4b • if the diagnosis and procedures have been flagged as confidential, the invoices are checked in the VAD rooms by auxiliaries of the medical examiner. These are the only persons who have access to the diagnosis and procedure data, from the time the data are received until they are archived. They check the obligation to pay benefits and inform Administration of their assessment. Invoices are always approved or rejected by Administration, who only has access to the invoice data.

5 • The statutory safekeeping period applies for electronic invoices and MCD data. After processing as defined by Art. 59a^{ter} para. 2 KVV, the MCD can only be accessed by the VAD.

ENCLOSURE 4

Data flow diagram (receipt by mail)



*Anforderung an Papiereingang und MCD-Erfassung: vollständig getrennt von Administration und VA

Explanations to data flow diagram (receipt by mail)

- 1 The mail is physically delivered in locked boxes by the postal service to the DAS at an agreed time.
- 2 / 3 The invoices and MCD are accepted and captured manually in the system. The documents addressed to the VAD are flagged in the system.
- 4 After capture, the MCD are temporarily filed at the DAS. The physical MCD are then stored in a VAD archive for the statutory safekeeping period. More information is provided in internal documents.
- 5 After the invoice has been captured, the DAS employee releases the invoice to allow its validation against the rules.
- 6 As soon as the invoice has been approved, it is physically sent on for scanning.
- 7 It is then validated against the rules. DRG invoices (incl. MCD) are accepted and decrypted. An insurance as well as a medical test is run. It is then sorted and forwarded to the competent units.
- 8 If the rules are satisfied and no discrepancies are identified, the invoice is automatically paid.
- 9 If the rules are not satisfied, the invoice is rejected and sent to Administration for checking, unless flagged for the VAD. Administration then manually checks the invoice.
- 10 If the rules are not satisfied for invoices flagged for the VAD, the invoice is rejected and sent to the VAD auxiliaries for further processing.
- 11 After capture by the DAS, the physical invoices are scanned and read into the system in rooms with access control. The physical invoices are then destroyed.

ENCLOSURE 5

Abbreviations

ATSG	Federal Act of 6 October 2000 on the General Part of Social Insurance Law (SR 830.1)
e.g.	for example
DAS	Data collection point pursuant to Art. 59a para. 3 KVV
DSG	Federal Act of 19 June 1992 on Data Protection (SR 235.1)
KVAG	Federal Act of 26 September 2014 on the Supervision of Social Health Insurance (SR 832.12)
KVG	Federal Health Insurance Act of 18 March 1994 (SR 832.10)
KVV	Ordinance of 27 June 1995 to the Federal Health Insurance Act (SR 832.102)
MCD	Minimal clinical dataset
USR	Corporate standards and guidelines
VAD	Medical examination service
VDSG	Ordinance of 14 June 1993 to the Federal Act on Data Protection (SR 235.11)

ENCLOSURE 6

Contact addresses

Requests for information, updates and deletion of data must be sent to:

Helsana Insurance Company Ltd
Data Protection Officer
P.O. Box
8081 Zurich

Specialist enquiries:

Helsana Insurance Company Ltd
Hospital and Nursing Care Specialist Department
P.O. Box
8081 Zurich