The contexts in which medical data are exchanged are increasing.

In the context of his "ownership" of a patient's general medical file (Dossier Médical Global or DMG) and the scaling of medical costs (Echelonnement), a general practitioner has responsibility for coordinating a patient's treatment. He therefore needs access to all information a patient wishes him to see.

Healthcare institutions, collaborations such as provided for under the Impulseo programmes, extended (health-)care centres in both urban and rural communities are requesting GPs to share relevant information to ensure the ongoing treatment of their patients.

Subject to increasing financial pressure, hospitals are having to reduce the length of stays and to give precedence to day-care. Pre- and post-operations check-ups are taking place on an outpatient basis, and patients are generally leaving hospital earlier and in a more fragile state. It is therefore essential that the data gathered in the course of hospital treatment be immediately accessible to those responsible for the follow-up treatment outside the hospital.

Hospitals themselves are becoming increasingly specialised, and they are now required to adopt a "Bassin de soins" strategy tailored to the healthcare needs of a specific region and in which inter-hospital transfers are necessary for specialised treatment.

The idea behind the Réseau Santé Wallon / RSW / Walloon eHealth Network is to provide an organisational and technological framework offering state-of-the-art security and standardisation to support the exchange of medical records between all health professionals at cost price, in compliance with medical ethics and patient privacy regulations. The RSW thus provides a technological solution inter alia avoiding the need to create a shared central health database.

One of the project's priorities is to improve the medical treatment of a patient by doctors of his choice, without excluding the economic and scientific benefits possibly deriving from such.

As a long-term project and given its cultural, organisational, technological and financial implications, it will be developed in a step-by-step and prudent manner.

Both its promoters and its users will never lose sight of the fact that it is being developed in the exclusive interest of patients, and that this takes precedence over any other consideration.
Informed patient consent is a sine qua non for enabling the exchange of records concerning the patient in question.

Similarly the explicit agreement of the health professional to abide by these Regulations is a sine qua non for giving him access to the system. His participation is free and voluntary. Only medical records relevant for ensuring the ongoing treatment of a patient will be exchanged, subject to the patient’s consent.

Patients retain full ownership of access rights to their records.

The RSW will never be able to claim to be able to provide a comprehensive view of a patient’s medical data.

The aim of this document is to define the rules governing the use of the RSW.

In it, patients will find the official response to the RSW's legal obligation to publish its regulations regarding data privacy.

Users of the system will find in it a reference guide allowing them to benefit from the system in respect of the basic principles of data privacy, data confidentiality and the non-disclosure of medical information, never forgetting that the sole raison d’être of the RSW is to promote the interests of patients.

Given that the RSW acts as a hub within the overall Belgian strategy of connecting up Belgian health systems, it also complies with the regulations applying to the national hub-meta hub project.

### Table of contents

Introduction..................................................................................................................................................1

§1. Definitions................................................................................................................................................3

§2. Description of the Réseau Santé Wallon (RSW)..................................................................................5

§3. Regulatory and legislative framework .................................................................................................8

§4. Purposes and legitimacy of processing the data....................................................................................10

§5. Data processing responsibility / subcontracting: ...............................................................................11

§6. Patient rights ........................................................................................................................................13

§7. Confidentiality and access rights........................................................................................................16

§8. Data security ........................................................................................................................................16

§9. Glossary (in the sense of the RSW) ........................................................................................................27
§1. Definitions

FRATEM

FRATEM stands for the "Fédération Régionale des Associations de Télématique Médicale", a non-profit organisation bringing together providers of health telematics in Wallonia and with its registered office at Rue de Hesbaye 75, 4000 LIEGE. It is registered under number 898.587.313.

The purpose of the association is: the study, organisation and implementation of all means allowing the best and lowest-cost communication possible between the different healthcare providers represented in Wallonia, and in particular the automated electronic transmission or provision by telematic means of all data or communications of medical relevance using the most appropriate technology, as well as - from a more general perspective - the transmission of messages of general interest (excluding all messages of an advertising nature). Though its work, it aims to boost the quality of the treatment administered to patients, without prejudice to the objectives and activities of local telematic associations (extract from the FRATEM statutes).

FRATEM is the official owner of the Réseau Santé Wallon / RSW, and is responsible for its funding, development, support and control. It is represented by its President.

The FRATEM statutes are available on www.rsw.be/statuts

The RSW Oversight Committee

An Oversight Committee has been set up to monitor compliance with legislation and with these Regulations. The Committee is a completely independent body responsible for permanently auditing the functioning of the RSW and issuing, whether on request or not, opinions or recommendations in matters of confidentiality, access rights, security and privacy to the FRATEM Management Board.

The independence of Oversight Committee members is guaranteed on the one hand by their external (i.e. non-FRATEM) designation and on the other hand by the fact that the persons serving on the committee must not be involved in the management of the RSW.

The Oversight Committee is made up of:
- one patient representative, designated by the League of Health Service Users / Ligue des Usagers des Services de Santé,
- one representative from the Federal Commission on Patient Rights,
- one doctor designated by the Ordre National des Médecins
- one doctor designated by the Académie Royale de Médecine
- one doctor designated by the Société Scientifique de Médecine Générale
- one doctor designated by the Association francophone des Médecins-chefs

The commission is assisted in its work by a legal specialist, an IT specialist and a delegate from FRATEM in a secretarial capacity. These three members sit in an advisory capacity, with the first two coming from the academic world.

The Committee is responsible for drawing up its own rules of procedure.

The current composition of the RSW Oversight Committee is available on www.rsw.be/comitesurveillance

Patient health data

The RSW manages the exchange of personal data related to a patient's health in the sense of the WHO: "Health is a state of complete physical, mental and social well-being and not merely the absence of disease or infirmity."

For purposes of simplicity, the term "patient health data" in this document is used to refer to all data of personal nature providing information on a previous, current or future state of physical or mental health of an identified or identifiable physical person, i.e. the patient, complemented by personal identification data supporting the treatment administered to the patient in question.

A distinction is made between
- a central database on the central server
- decentralised databases on the source systems (typically in hospitals)
The central database contains:

- patient identification data and their declarations of consent
- health professional identification data and their registration details
- the index for medical records referenced on the central server
- copies of "emergency health records" ("sumehr")
- certain health data that service providers without online servers wish to share
- the logs of access rights and accesses

As the RSW is responsible for organising the exchange of medical records, health professionals are forbidden from inserting any personal annotations, as this would mean that a record would de facto lose its status. The RSW therefore does not transport any personal annotations in the sense of the law on patient rights.

**Sumehr (Summarised Electronic Healthcare Record/emergency health record)**

The **Sumehr** is to be seen as a "health photo of the patient" - a snapshot that the treating doctor, in his capacity as manager of the Comprehensive Medical File / Dossier Médical Global / DMG, takes during his privileged contacts with the patient. For from being static, the "Sumehr" evolves in line with the patient's state of health. It is not to be seen as a full health file, but as an extract thereof containing health details of use for future treatment.

**Health IT system / Dossier médical informatisé (DMI)**

In the context of this document, this refers to any system allowing a patient's health data to be viewed or managed. For simplicity, we will use the term DMIG when referring to a GP's system and DMIH when referring to a hospital system. However, by analogy other systems can also be taken into account, including laboratory data servers, specialised gynaecology software, a physiotherapy database, a simple viewing tool using a smartphone, etc.

Typically, a DMIH stores its own data, but provides access thereto via the RSW. Typically, a DMIG only provides access though storing a copy of its data on the RSW.

An **approved DMI** is a DMI whose integration into the RSW has been certified by the latter, though this has no direct link to the Federal certification process.

Only approved DMIs may link up to the RSW.
§2. Description of the Réseau Santé Wallon (RSW)

Introduction

The RSW is a data communications infrastructure allowing the exchange of medical records between health professionals, in the context of the ongoing treatment of their patients. A medical record can be anything from a consultation report, a lab report or a hospitalisation report to an emergency health record.

The RSW is against the central storage of all medical records, with each health professional using his own system (DMI), with which he can access relevant records to which other health professionals have given him access in consultation with the patient and with the latter's consent.

Functionality of the RSW

The RSW provides

- an explicit regulatory framework
- an organisational framework ensuring
  - the design, development, roll-out and support of technical tools
  - training and support for users of the system, whether patients or health professionals
  - the organisation of an independent supervisory structure
- a technical platform allowing the efficient and secure exchange of medical records relevant to the ongoing treatment of patients. This platform is based on 3 main modules;
  - RSW\Hub: the set of functions enabling the interconnection of the systems (DMIs) of health professionals both within and outside hospitals, thereby acting as a hub in the overall framework of the Belgian hub-metahub project
  - RSW\Inter-Med: a secure structure for hosting health records for health professionals without their own online servers
  - RSW\Mail: tools allowing the exchange of secure messages between health professionals

The technical platform

To ensure the interconnectivity of approved DMIs, the RSW\Hub module offers the following tools:

- a secure central server hosting the data described in the simplified diagram of the RSW below
- a secure connection infrastructure between hospital DMIs (DM Ih) and the central server
- a secure connection infrastructure between the DMIs of individual doctors (non-hospital) (DM Ig) and the central server
- mechanisms for registering patients and managing their declarations of consent
- mechanisms for registering health professionals and managing their registration details
- mechanisms for managing access rights, based on the existence of a therapeutic link between the patient and the health professional, and allowing the management of exceptions at health professional or document level
- mechanisms for logging accesses and viewing such logs
- mechanisms for electronically signing transactions carried out over the network
- the establishment of a secure index of patients having given their consent to sharing some or all of their records
- the establishment of a secure index of records authorised for sharing, sourced by approved DMIs
- the provision of a web service allowing the medical record index to be read for a specific patient
- the provision of a web service allowing a given record to be viewed, downloaded
- the provision of mechanisms restricting the dissemination of a specific record or managing a list of approved recipients for such

In the context of the federal Hub-Metahub structure, the RSW also adheres to federal-level specifications allowing exchanges between hubs. All exchanges are standardised using the Kmehr format (including the Kmehr web services), thereby ensuring maximum compatibility with the Brussels and Flemish eHealth networks and general practice DMIs.

The use of Inter-Med is restricted to data relevant for sharing information in the context of outpatient treatment. In consultation with the patient, the treating doctor can place a summary file (the so-called "sumehr") or other relevant health data in the RSW\Inter-Med module. In such a case an entry is made in the RSW index, while the record is physically stored in the RSW/Inter-Med "safe". Such record storage also requires the definition of access rules. Such data can then be viewed by other health professionals in consultation with the patient, thereby ensuring better treatment, for example in emergencies.
RSW\Mail includes various tools allowing the exchange of secure messages between health professionals. The RSW\Mail module's system of mail notifications covers the management of the recipients of an indexed or stored record, the management of "have-read" acknowledgements, the possibility for a DMI to access the list of records to be read for viewing or download purposes, as well as a system of alerts.

The RSW also provides a secure portal allowing professionals without an approved DMI to view the records of their patients. It also allows patients to track and manage access rights to their records.

**RSW users**

The RSW distinguishes between the following users

- a Patient
- a Health Professional
- an Administrator
- an IT Administrator
- a Local Administrator

A Patient is any person for whom medical records are or have been potentially exchangeable following the informed consent of the patient himself or of his legal representative.

A Health Professional is any professional in the sense of Royal Decree No 78 of 10 November 1967 on the exercise of healthcare professions and who participates in the ongoing treatment of a patient - i.e. he is involved in the diagnosis or treatment or in any preventive measures regarding individual patients.

Administrators are FRATEM employees responsible for performing certain administrative tasks at the request of patients, health professionals or the Oversight Committee.

IT Administrators are FRATEM employees responsible for performing certain technical tasks regarding the central IT system such as maintenance work on the network, the server farm or updating applications.

Local Administrators are persons designated by an institution sourcing decentralised records (typically a hospital) who,
under the responsibility of the data processing manager, work in consultation with the FRATEM (IT) Administrators to prevent/resolve any problems involving the interconnection of DMIs with the central server.

Explicit acceptance of these Date Privacy Regulations is a sine qua non condition for becoming an RSW user. This signed declaration of acceptance needs to be stored within the RSW before access can be enabled. As a result of deliberation 12-047 of the Date Privacy Commission, a patient's physical signature is no longer required insofar as his National Citizen Registration Number (numéro national) and the number of his electronic ID card (eID) are stored. As regards the site sourcing decentralised records, a formal contract defines its relationship with FRATEM.

**RSW administration**

In the context of its administration remit, FRATEM is responsible for the following:

- Publication and distribution of the RSW Regulations
- Management and supervision of patient registrations, declarations of consent and revocations
- Management of user health professional registrations, accreditations and revocations
- Management of access authorisations to all or part of a patient's records
- Communicating to patients the history (log) of accesses to his records
- Communicating to patients a copy of the data stored centrally (on request)
- General support for system users

In the context of its IT management, FRATEM mobilises IT skills necessary for fulfilling the following objectives:

- Development of applications and services
- Development of services targeting users
- Network and server maintenance

The persons designated by FRATEM to perform these administrative and IT management tasks all need to officially sign a non-disclosure agreement. They have no right of access to the health records of patients, except in cases where patients specifically accord them such a right or in the specific context of their work.

**RSW Ombudsman**

FRATEM appoints an ombudsman whose job it is to identify and investigate all complaints in a fully independent capacity. Reporting directly to FRATEM,

the Ombudsman has the following tasks:

- Acknowledgement and investigation of complaints related to the use of the RSW network (with the exception of problems relating to decentralised data)
- Finding solutions satisfactory to all parties
- Submitting an annual report to the FRATEM Management Board and the Oversight Committee

The Ombudsman has the option of involving the Oversight Committee when he considers this to be appropriate.
§3. Regulatory and legislative framework

This document describes how the RSW complies with the legal provisions and ethical principles governing the management of health records. In more concrete terms, it describes how it fulfils the following:

- the obligations set forth in the Belgian Data Privacy Act of 8 December 1992 with regard to:
  - the legitimacy of processing data of a personal nature
  - the explicit description of the purpose thereof
  - responsibility for processing the data
  - the duration data is stored
  - the rights of the person concerned
  - confidentiality
  - data security and quality
  - making known how data of a personal nature are processed

- the obligations set forth in the Royal Decree of 13 February 2001 on the implementation of the Data Privacy Act with regard to the coding or anonymisation of data in the context of analysing them for historical, statistical and scientific purposes departing from the original processing purpose.

- the obligations set forth in the Law on Patient Rights of 22 August 2002, with a specific focus on the modalities regarding a patient’s access to his medical records, to personal annotations of doctors to medical records and to data relating to third parties

- the provisions of the Law of 13 December 2006 on various provisions in the health field, including:
  - The Sectoral Social Security and Health Data Committee
  - the authorisations to be obtained from this Committee

- professional secrecy (Art. 458 of the Criminal Code)

- the Medical Ethics Code, and more specifically the recommendations issued by the Medical Association (Ordre des Médecins) on 17 October 2005 on medical databases containing personal or identifiable data; the opinion of 27 July 2003 on the Law on Patient Rights; and opinion of 20 January 2007 on patients being allowed to directly view their electronic medical records.

- the Law of 8 August 1983 setting up a National Citizen Register

- the Law of 17 July 1990 setting up the Banque Carrefour de la Sécurité Sociale.

- the Law of 9 July 2001 setting certain rules regarding the legal framework for electronic signatures and certification services

- The WP131 working document of the Article 29 working group, set up by European Directive 95/46/EC, on the processing of personal data related to health contained in electronic medical records (EMR), adopted on 15 February 2007 and specifically stating that the “direct exchange of medical records helps improve healthcare quality ....”.

- the Law of 20 October 2000 on IT criminality

- the inviolability of communications (Article 314.a of the Criminal Code)

- standard practices regarding the protection of personal data, published by the Data Privacy Commission.

- Deliberation 12/047 of the Health Section of Sectoral Social Security Committee based in particular on the deliberations related to:
  - the “Regulations for the general functioning of the hubs & metahub system” (in association with Deliberation 11/089 of the Sectoral Health Committee).
  - the informed consent of the patient: (in accordance with Deliberation 11/046 of the Health Section of the Sectoral Social Security Committee)
  - proof of the therapeutic relationship: (in accordance with Deliberation 11/088 of the Health Section of the Sectoral Social Security Committee)
• The Law of 21 August 2008 on the establishment and organisation of the eHealth platform and the associated royal decrees implementing it
§4. Purposes and legitimacy of processing the data

The computerisation of medical records, when well designed and complying with data security and privacy norms, has the ability to improve a doctor's work, to facilitate the exchange of relevant information between health professionals, to avoid the unnecessary duplication of medical examinations - all for the benefit of the patient. Yet only this last consideration really justifies project implementation.

Extract from the opinion of the Belgian Royal Academy of Medicine of 13 February 2007.

The DME (Dossier Médical Electronique / Electronic Medical File) is presented as an appropriate means of:
• improving treatment quality through having better data on a patient;
• improving the cost-efficiency of medical treatment and thus curbing the rapid increase in health budget deficits;
• providing data necessary for quality control, statistics and planning in the public health sector, which should also have positive effects on public health budgets.

Extract from WP131, the Working Document on the processing of personal health-related data contained in electronic medical databases (15 February 2007).

Exchange of medical records in the context of ongoing treatment

The RSW is responsible for organising the exchange of medical records between health professionals by the secure interconnection of their IT systems/databases (DMIs).

This exchange of medical records is only to be used for improving the quality of the medical treatment of individual patients.

Only health professionals participating in the ongoing treatment of a patient, i.e. activities involving diagnosis, treatment or prevention, have access to these records.

The exchange of a patient's medical records is dependent on his informed consent being given beforehand. Such consent is explicitly authorised by Deliberation 12/047 of the Data Privacy Commission.

The RSW stores only the minimum of data needed to accomplish its mission: patient and health professional identification data, the indices of available records, access rights, access logs. The actual medical records remain stored on the servers of the institutions actually sourcing the data (typically hospitals). The RSW allows health professionals without their own servers (typically GPs) to store their treatment data in the RSW\Inter-Med safe store. These typically include the summarised electronic health record (the "sumehr").

Restrictions

It is forbidden for any health professional to access health data using the RSW for any reason other than for providing ongoing treatment. Prohibited purposes include expert assessments, insurance contracts, or eligibility for refunds.

The RSW prohibits any capability of directly analysing its data for scientific or business purposes.

Where a request is made by a public or scientific body to analyse the data, the latter will be made available in an irreversibly anonymised form, and only after authorisation by the FRATEM Management Board and the Data Privacy Commission.

In addition, it should be remembered that the RSW has no intention of becoming the repository for the full medical file of a patient. Moreover this is basically not possible as:
• the participation of health professionals is voluntary
• only records relevant to ongoing treatment are exchanged within the network
• patients have the right to select which records / which professionals are excluded from such exchange.
§5. Data processing responsibility / subcontracting:

In the context of medical records

Who is responsible for processing data?

Within the RSW the body responsible for processing data is each individual healthcare institution or each health professional defined as a user.

Each body responsible for processing date must submit an individual declaration to the Data Privacy Commission.

Subcontracting

RSW management is in the hands of FRATEM, an organisation acting as a subcontractor with regard to the data within the medical records exchanged.

By its nature, the RSW brings together input from a wide range of data centres. As a subcontractor it thus has to perform certain administrative operations on behalf of the latter, by explicit delegation.

The subcontractor has responsibility for designating:

- a health professional responsible for overseeing the processing of this data,
- a security consultant with regard to the organisational and technical security measures, who carries out his work in an independent manner,
- an ombudsman.

In the context of managing the IDs of individuals

In performing its work as a subcontractor, FRATEM manages individual IDs within the RSW, for both patients and health professionals. These IDs are unique and specific to the RSW. They are generated using a reversible encryption algorithm based on the National Citizen Registration Number.

FRATEM is responsible for this application. After having gained the agreement of its sectoral “national register” committee, it submitted a data privacy declaration to this effect to the Data Privacy Commission.

Data processing declaration

Each healthcare institution or health professional defined as being responsible for processing a patient's health records via the RSW must declare such processing to the Data Privacy Commission. This declaration can be made online at the following address: http://www.privacycommission.be/fr.

FRATEM's declaration regarding the processing of data related to the National Citizen Registration Number can be found under the reference [1275501768512].

These Regulations are available on the Internet at the following address: www.rsw.be/reglementvieprivee
A paper version can be requested from FRATEM, Rue de Hesbaye 75, 4000 LIEGE.

Only users having declared their informed consent to these Regulations may access the system. Declarations of consent are stored in digital form on the RSW.

Back-up period

The subcontractor guarantees the back-up of centrally-held data for a period of 30 years from the last transaction made with regard to the patient.

Centrally-held data include:

- patient identification data and patients' declarations of consent
- health professionals identification data and their registration and accreditation details
- the index of the records indexed on the central server
- copies of the summary electronic health record (emergency health record) and other health data
- the history (logs) of access rights and that of data accesses.
Beyond this period, the subcontractor reserves the right to destroy the information without notice.

The RSW reminds each health professional of his own data back-up responsibilities with regard to decentralised data; i.e. medical records stored for the most part in the systems (DMIs) of these professionals.
§6. Patient rights

Information and consent of patients for processing their data

The Data Privacy Act explicitly sets forth the rights of the person concerned with regard to the processing of his personal data. This law is complemented by the specific Patient Rights Act with its focus on medical records.

A patient has the right to know which data / records have been recorded or communicated, why, by whom and how. These Regulations constitute a first response to this requirement. For more detailed information, a patient may submit an official signed and dated request to the person or institution responsible for the processing. A response must be communicated to him within the statutory time limit - i.e. no longer than 45 days after receipt of the request.

These Regulations respond to a patient's rights with regard to the identification of the person or institution responsible for the processing, his rights and the persons or categories of persons authorised to access his health data.

However the following provisions only relate to the data held centrally by the RSW, i.e. the summarised electronic health records (“sumehr”) and data related to the organisation of data exchange.

To view or modify decentralised data, the patient needs to contact the person or institution responsible for processing the data of these decentralised systems (typically the hospitals).

The right to view one's data

A patient may view the data relating to his person. As regards access to medical records, this access is restricted in 2013 to persons involved in a pilot project and having given their explicit consent. The aim of this project is to define the practical modalities of such access in consultation with the public health authorities (SPF Santé Publique).

It is to be seen as an opportunity to improve the dialogue and to enhance the role of patients in the context of their treatment.

Patients have available several channels for accessing data concerning them, dependent on the nature of the data.

<table>
<thead>
<tr>
<th>Nature of the data</th>
<th>Access channel</th>
<th>Time limit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access authorisations associated with patients</td>
<td>Direct access by a patient via Internet, using his electronic ID card and PIN code <a href="http://www.rsw.be">www.rsw.be</a></td>
<td>Provisional solution</td>
</tr>
<tr>
<td>Log of which health professionals have accessed a patient's records</td>
<td>The patient asks the health professional of his choice. The latter must be registered with the RSW and must be authorised to access the patient's records. Submit a written request to the subcontractor, who will act by delegation.</td>
<td>Under the responsibility of the health professional to whom the patient addresses his request. Paper reply within 15 working days.</td>
</tr>
</tbody>
</table>

Detailed history of accesses to the patient's records. List of records available

<table>
<thead>
<tr>
<th>Nature of the data</th>
<th>Access channel</th>
<th>Time limit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Direct access by a patient via Internet, using his electronic ID card and PIN code <a href="http://www.rsw.be">www.rsw.be</a></td>
<td>Provisional solution</td>
<td></td>
</tr>
<tr>
<td>The patient asks the health professional of his choice. The latter must be registered with the RSW and must be authorised to access the patient's records. Submit a written request to the subcontractor, who will act by delegation.</td>
<td>Under the responsibility of the health professional to whom the patient addresses his request. Paper reply within 15 working days.</td>
<td></td>
</tr>
</tbody>
</table>

Last update: 01/03/2013
<table>
<thead>
<tr>
<th>Viewing the Summarised Electronic Health Record (&quot;Sumehr&quot;) and decentralised data in the RSW &quot;safe&quot;</th>
<th>Direct access by a patient via Internet, using his electronic ID card and PIN code: <a href="http://www.rsw.be">www.rsw.be</a></th>
<th>This access is restricted in 2013 to persons involved in a pilot project and having given their explicit consent. The aim of this project is to define the practical modalities of such access in consultation with the public health authorities (SPF Santé Publique).</th>
</tr>
</thead>
<tbody>
<tr>
<td>The patient asks the health professional of his choice. The latter must be registered with the RSW and must be authorised to access the patient’s records. Ideally, the patient will ask the doctor responsible for compiling the Summarised Electronic Health Record (&quot;Sumehr&quot;) (typically his GP).</td>
<td>Under the responsibility of the health professional to whom the patient addresses his request.</td>
<td></td>
</tr>
<tr>
<td>Submit a written request to the subcontractor, who will act by delegation.</td>
<td>Paper reply within 15 working days.</td>
<td></td>
</tr>
<tr>
<td>Decentralised data</td>
<td>Direct access by a patient via Internet, using his electronic ID card and PIN code: <a href="http://www.rsw.be">www.rsw.be</a></td>
<td>This is outside the scope of the RSW.</td>
</tr>
<tr>
<td>Patients need to contact the person or institution responsible for the decentralised system (typically the system of a hospital).</td>
<td>This access is restricted in 2013 to persons involved in a pilot project. The aim of this project is to define the practical modalities of such access in consultation with the public health authorities (SPF Santé Publique). Only records sourced by hospitals and doctors participating in the pilot project will be accessible.</td>
<td></td>
</tr>
</tbody>
</table>

It is recommended that the health professional asked goes through the file with the patient, providing any explanations the latter may want.

Subject to the conditions foreseen under the law, the relatives (up to 2nd degree) of a deceased patient may demand access to the centralised RSW data, insofar that the patient did not restrict their access during his lifetime. Such access is only possible via a health professional. Such requests must be sufficiently justified and specified.

**Right of rectification / correction**

The Data Privacy Act similarly foresees that the person concerned may, under certain conditions, have his personal data corrected, or even deleted, free of charge. Such action can relate to incorrect data, or to data which the patient judges to be unrelated to the purpose of treatment. We would like to remind readers that the vast majority of data is held in decentralised systems and that their correction is thus not within the responsibility of the RSW. Should a patient’s medical data need to be modified within the RSW, the patient should discuss this first with the health professional responsible for having the data filed. If no agreement can be reached, a dated and signed request should be submitted to the subcontractor; the correction will then be made by the health professional responsible for the data in the following month.

However, in cases where it appears that such changes could have a negative effect on the other legitimate purposes of the treatment, including the correct medical follow-up of the patient or archiving for medico-legal reasons, the healthcare professional may oppose such a change. The contested data should then be immediately reported as such to the RSW, pending resolution of the dispute.

**Right to a copy of the data**

Last update: 01/03/2013
Patients may obtain an intelligible copy of his central data at cost price, subject to the conditions set out in the context of viewing such data. A written request, signed and dated, must be submitted to the subcontractor. It will be processed within 15 working days. The copy is to be explicitly stamped as being strictly personal and confidential.

**Intervention of a trusted person**

The patient can designate a trusted person of his choice who will support him or act on his behalf when viewing his RSW data, or requesting or obtaining a copy thereof. The identity of this person will be kept on the files at the RSW (a section is foreseen for such data in the patient’s identification record). Health professionals will regularly ask patients whether the information remains relevant.

**Intervention of a doctor chosen by the patient**

To view a patient's medical records via the RSW, the patient's trusted person must be a doctor in the following situation: if the doctor sourcing the record has judged that the patient should not access the data in his own medical interest, pursuant to Article 7 §4 of the Patient Rights Act.

**Intervention of the patient's legal representative**

When the patient is incapable of exercising his rights (a minor not in a position to reasonably assess his interests, a person in a coma, etc.), his legal representative has the right to exercise the patient's rights pursuant to Articles 12 - 14 of the Patient Rights Act, subject to the requests for information being in the exclusive interest of the patient. The representative must have been designated beforehand and in writing by the patient (obligatory in the sense of Article 14 §1 of the Patient Rights Act. Such designation must be recorded in the patient's identification record at the RSW. By default, it is defined by law.

For minors, the health professional can refuse the child's legal representative's access to the central records when he deems that the minor is sufficiently capable of deciding the contrary.

Pursuant to Article 15 of the Patient Rights Act and with a view to protecting a patient's privacy, a health professional can refuse access to a patient's medical records.

**Resolution of disputes related to the application of patient rights**

In the event of a conflict arising between the patient and the health professional to whom the request is submitted when applying the above-mentioned rules, we recommend submitting the dispute to the FRATEM ombudsman. The ombudsman is responsible for finding a solution satisfactory to all parties.

In the event of this procedure not being successful, the patient can submit an official complaint to the RSW's Oversight Committee.

In the event of this also being unsuccessful, the patient has the option of turning to the Federal department responsible for mediating in patient right disputes, to the Data Privacy Commission, or to the president of his local court. Belgian courts have jurisdiction to settle differences between parties. For foreign patients, the dispute must be submitted to the Tribunal de Liège.
§7. Confidentiality and access rights

Preliminary comments

The RSW does not modify the nature of data exchanges within the Walloon region. Its job is to facilitate such exchanges, to enable their standardisation and to speed them up, against a background of minimal centralised storage of medical records.

In reality,
- all hospitals, private labs and a large number of specialists already communicate the records of their patients by electronic means,
- a number of hospitals already allow GPs to access their patients' records via the Internet,
- the records exchanged by the RSW remain on their source systems, with the exception of the summarised electronic health record ("sumehr"); there is thus no actual physical file centralising all the records of a patient,
- the RSW operates a ban on any capabilities to analyse the data exchanged.

The specific purpose of the Réseau Santé Wallon is to provide a common technical and organisational architecture allowing all health professionals in Wallonia to exchange their medical records electronically and in a standardised manner. This opens up the possibility of accessing patient records via hospital software systems, irrespective of where the records are actually stored, thus improving the quality of exchanges and potentially boosting the quality of patient care.

Economies of scale allow all health professionals to benefit from a stronger infrastructure and tighter regulations.

Though it is obvious that such a network presents new risks (potential larger-scale accesses), the system is equipped with strong technological firewalls and other barriers greatly restricting access to the records, as well as with a system systematically logging all accesses. Moreover, the system offers better guarantees than the current paper-based system: no mix-ups, the possibility for patients to limit access to their records and to view the index of their records. In a future phase, patients should be able to directly access their records and thus contribute to validating them.

Basic principles

There are a number of basic principles governing access to a patient's medical records via the RSW:
- There is a ban on accessing a patient's records in situations not directly related to achieving or supporting one of the system's described purposes. In this context, a health professional accessing a patient's records must only access those records needed for carrying out his work; and only during the period required for its execution.
- All persons accessing patient records are bound to the rules of non-disclosure (professional secrecy). No data can be communicated to third parties in any form without the explicit consent of the patient.
- Access to patient records must always be justified by the exclusive interest of the patient.
- The RSW cannot be used for communicating personal notes. Their exchange would lead to them de facto losing this status.
- Alongside adhering to these ethical rules which health professionals pledge to respect when registering with the RSW, specific functions are incorporated into the system and allowing patients to control and limit access to their records, and logging accesses.
- Data marked as psychiatric or genetic is only accessible to health professionals with explicit accreditation for these specific fields.
- A patient may draw up a list of health professionals for whom he denies access to his records. To do this, a patient can either enter such a list himself, or can have himself helped by a trusted person, a legal representative or by a doctor with access to his records - such as his treating doctor. A patient or his legal representative may also submit a written request to the RSW administrator, based at the FRATEM headquarters.
- For each record in his file, a patient can either limit access to a list of health professionals (i.e. only those in the list have access) or ban a list of health professionals from access. In the latter case records remain accessible to other health professionals with an active therapeutic link and ad hoc accreditations. Access modalities are the same as those described above.
- All record accesses are logged in a non-modifiable file. This may be viewed, at a patient's specific request, by any health professional with access authorisation to the patient's records or by the health professional responsible for monitoring the RSW. Patients also have access to this information under the same modalities described above. Any abuse is subject to strict legal and disciplinary sanctions.
- In the case of any dispute, patients may call on the services of an ombudsman provided by the RSW, or even
Introduction to access right management

The objective here is to define whether a health professional has permission (may or may not) to carry out a certain action (view, for example) on an object (hospitalisation report, for example) for a given patient, dependent on a certain context (treating doctor, on-call doctor, for example).

For permission to be given, the following is required:
1. The patient or his legal representative must have given explicit consent to his records being exchanged via the RSW.
2. A health professional (source professional) must have declared the record as being relevant for exchange.
3. This declaration must not be associated with a general or specific exclusion of the receiving professional.
4. The receiving professional must have explicitly declared his agreement to abide by the RSW Regulations.
5. The receiving professional must have the right to carry out the action (view) on objects of this category (specific rights required - for instance - for psychiatric or genetic records).
6. The receiving professional must have legitimised his access to this patient's records (the treating doctor or an emergency for example).

The principles behind the management of patient rights within the RSW stem from the OrBAC (organization-based access control) model, the most advanced model for managing access rights in the medical world. Nevertheless, the system operated by the RSW is much more stereotyped than a normal shared medical file in a hospital, for the following reasons:

- generally speaking only records (and very few structured data) are exchanged
- the only structured records exchanged are summary records
- there is no grouping of data (summary charts for example)
- the scope of actions allowed is very limited (basically just declaring or viewing documents).

The OrBAC model actually implemented is consequently greatly simplified, even though each of its concepts has been faithfully reproduced in the RSW.

We will now go on to describe the following mechanisms:

- Managing a patient's consent
- Managing the registration and accreditation of a health professional
- Publishing a record (the responsibility of a health professional)
- Deleting a record
- Prohibiting a health professional from access
- Prohibiting access to a specific record
- Managing access authorisations
- Access right levels
- Managing user profiles
- Assigning access rights
- Tracking (logging) accesses

Patient consent

Medical records cannot be exchanged without the prior informed consent of the patient. This process of giving consent takes place in two steps: a) patient registration; b) declaration of consent.

1. Patient registration
The aim of this step is to register a patient's basic person-related data. It involves assigning a regional (Walloon) health number derived from the National Citizen Registration Number. Only this regional ID is stored and communicated within the RSW.

Registration can be done in a number of ways:
- directly by the patient via the registration form available on the Internet
by any doctor, using either the same form or via exporting the data from his DMIg system
by a hospital (or similar institution) via exporting the data from its DMIh system
by the RSW administration on the basis of a patient's written request.

2. **A patient's free and informed declaration of consent**

For registration to come into effect, the patient must explicitly declare his informed consent to the RSW Regulations. Such declaration can be made:

- via the Internet through a patient electronically signing the declaration by means of his electronic ID card (at home, at a GP's surgery, or any other place);
- or through manually signing the paper form (the signed form must then be sent to the RSW administration. The latter will in turn activate registration once the form has been scanned in and made available to all RSW members).
- or through manually signing the paper form within a hospital (or similar institution). In this case, the DMIh system declares the consent to the RSW, scans and archives the signed form, and informs the RSW of such.
- or - in accordance with Deliberation 11/047 of the Health Section of the Sectoral Social Security Committee -, the informed declaration of consent can be registered by a doctor, a chemist, a hospital or a health insurance. In this case, the social security ID number of the person concerned as well as the number of the patient's electronic ID card or his SIS card must be communicated to the RSW administration.

The patient will remain unknown within the data exchange system until he officially declares his consent to the RSW for his data to be exchanged.

With the ABRUMET\Net project of the Brussels-Capital Region being identical (same technical and regulatory conditions) to the RSW, a declaration of consent made in either region applies to both systems (they also have a very similar data privacy policy).

---

**Integration in the national hub-metahub project**

The national eHealth platform proposed managing a single consent system covering all medical record exchanges throughout Belgium. This approach was approved by the Health Section of the Sectoral Social Security Committee in its opinion 12/047. Patients can now also declare their consent on the eHealth website: [https://www.ehealth.fgov.be/login/login_citizen_eic_fr](https://www.ehealth.fgov.be/login/login_citizen_eic_fr)

Patients declaring their consent at national level authorise the RSW to allow access to their health records to all agents registered on the eHealth platform and pursuant to the modalities defined by it. As the RSW is not involved in the (already passed or future) decisions of the national eHealth platform, it cannot be held responsible for the disclosure of information pursuant to the latter's policies.

As for the declaration of consent registered with the RSW, this limits access scope to the agents and purposes described in these Regulations. Should the patient wish to extend his consent to a national level, he needs to declare his consent at this level. RSW agents are requested to suggest 2-level registration. Similarly the RSW website will also suggest this option to patients.

---

**Scope of consent**

In accordance with Deliberation 12/047 of the Health Section of the Sectoral Social Security Committee, a patient's consent applies to all past and future records. Healthcare providers remain free to publish past records.

**Revocation of patient registration**

A patient may revoke his registration at any time:

- directly via the Internet;
- or via his treating doctor,
- or via a request transferred to the RSW by the DMIh system
- or via sending the respective form to the RSW administration. Revocation comes into effect once the administration has processed the request.

The system also contains a function allowing notification of a patient's death; this results in the access rights to his records being modified in accordance with the Law.

---

**Integration into the national hub-metahub project**

With the RSW declaration of consent not having the same scope as that of a national one, revocation similarly needs to
**Patient monitoring of access rights**

The ways accesses are open to health professionals is explained a little later.

Suffice it to be said at this juncture that a patient may use the Internet to access the list of health professionals having accessed his records. He may also obtain such a list, or more detailed information, from the RSW administration; or via a health professional of his choice.

The patient can also prohibit access to all his records by one (or more) health professional(s):
- directly via the Internet,
- or by submitting a written request to the RSW administration,
- or by contacting a health professional of his choice who is able to carry out such an operation on the RSW.

Similarly a patient may prohibit one (or many) of his records being made available directly via the Internet, by contacting the RSW administration, or via a health professional of his choice. Ideally this decision should be communicated in advance to the doctor sourcing the record, meaning that it is then not declared.

Health professionals authorised to access a patient's records will have access to functions restricting access by other professionals to some or all records. He will only carry out such operations at the express request of the patient.

Patient functions are accessible via www.rsw.be via the patient's electronic ID card.

**Health professional registration**

Only health professionals having explicitly registered their agreement to abide by the RSW Regulations and who have RSW accreditation have access to the system.

**Professionals concerned**

In a first phase, use of the RSW will be restricted to doctors. In a later phase it will be extended to other health professionals.

Given the project's purpose, only people involved in the ongoing treatment of patients are considered as health professionals.

**Health professional registration/accreditation/revocation**

To become part of the RSW, a health professional needs to declare his processing of data to the Data Privacy Commission. For professionals working in a hospital or similar institution, this declaration is done by the latter. The health professional then needs to fill out an application form on the Internet, electronically sign his request for registration and designate on it a doctor vouching for him from amidst the health professionals recognised as such by FRATEM. The vouching doctor electronically approves the application, thereby completing registration, after having checked that the health professional works in the context of the objectives of the RSW. The health professional thus becomes accredited in the sense of the RSW.

The RSW administration can revoke a health professional's registration in the case of a breach of these Regulations being ascertained.

Health professionals can correct/modify their identification data at any time.

Last update: 01/03/2013
These functions are available to a health professional under www.rsw.be using his electronic ID card.

Participation in the project is voluntary. The RSW can never guarantee that all records pertaining to a certain patient are available on the network. Though there is a general wish that the summarized electronic health record ("sumehr") be made available by a patient's GP, there is no obligation to do so.

**Publishing a medical record**

Any accredited health professional may, in agreement with a patient who has registered his declaration of consent with the RSW, decide to "publish" a record on the RSW. In doing so, he needs to take care that only records relevant to ongoing treatment are made available. The health professional involved carries out such an action in the context of a secret shared with other health professionals who themselves have undertaken only to access the information in the very restrictive context of these Regulations going beyond the simple existence of a therapeutic link with the patient.

The publication of a record may be accompanied by restrictions on its disclosure: any health professional may, in consultation with the patient, either authorise or prohibit access to the record to a precise list of health professionals.

The health professional publicising the record has the right to access this record, insofar as he possesses an active therapeutic link to the patient and within the limits of the back-up rules.

**Deleting a reference to a record**

Records or references to them can be deactivated in the case of an error or at the request of a patient.

**Prohibiting access by a health professional to a patient's records**

A patient may prohibit access by a specific health professional to his medical records. To do this, he can do one of the following:

- carry out this operation himself via the RSW's patient portal,
- contact a health professional entitled to carry out this action on behalf of the patient,
- fill out an ad hoc form available under www.rsw.be (FAQ - administrative questions) and send it to the RSW administration. On this form, the patient can list health professionals for whom he wishes to prohibit access to his records via the RSW.

There is a function available enabling RSW administrators or any other health professional mandated by the patient to prohibit the access of a health professional to a patient's centralised records. This prohibition is accomplished via a 'negative access' for a certain period, and which cancels all existing authorisations for the patient/professional link.

**Integration in the national hub-metahub project**

The RSW is going to be fully synchronised with the national eHealth platform in this area. Exclusions of professionals can be implemented either via the RSW or via the eHealth platform; they will have the same effect of blocking the access of the health professional in question to records available on the RSW. This prohibition can be lifted via the eHealth platform or the RSW without distinction.

**Prohibiting access to a specific record**

Patients may prohibit access to one (or many) specific record(s) concerning his person. To deactive these records, a patient may:

- carry out this operation himself via the RSW's patient portal,
- contact a health professional entitled to carry out this action on behalf of the patient,
- fill out an ad hoc form available under www.rsw.be (FAQ - administrative questions) and send it to the RSW administration.

On this form, the patient can list (in free text) for which records he wants access via the RSW to be restricted.

There is a function available enabling RSW administrators or any other health professional mandated by the patient to prohibit the access of one, several or all health professionals to a patient's record(s). Using the list of an active patient's records as a base, one can either cancel access for all professionals or for a list of professionals selected using an interactive search form. There are facilities available for performing this function on a group of records.
Managing access authorisations

The intention of the RSW is to successively open up the network to different health professionals and to arrange the sharing of further types of health records. Against this background, the data access matrix by health professional is listed in the annex. It will evolve over time.

Below are a few examples of access authorisations involving doctors:

<table>
<thead>
<tr>
<th>Type of authorisation</th>
<th>Default time limit</th>
</tr>
</thead>
<tbody>
<tr>
<td>doctor treating the patient</td>
<td>unlimited duration (or until revocation)</td>
</tr>
<tr>
<td>ad hoc outpatient treatment</td>
<td>three months (renewed on each new contact)</td>
</tr>
<tr>
<td>ad hoc hospital treatment</td>
<td>three months (renewed on each new contact)</td>
</tr>
<tr>
<td>emergency treatment</td>
<td>duration limited to one month for such reasons as long weekends, medical controls and arbitration.</td>
</tr>
</tbody>
</table>

Patient access to medical records is restricted in 2013 to persons involved in a pilot project and having given their explicit consent. The aim of this project is to define the practical modalities of such access in consultation with the public health authorities (SPF Santé Publique).

Assignment of access rights

The rights to access RSW functions are assigned to user profiles by RSW administrators.

The following modalities apply when creating an access authorisation:

- In a non-hospital environment, creation by a health professional requires the patient's electronic ID card (or that of his legal representative) to be read. This technical requirement is one of the criteria for the approval of a DMI system.
- In a hospital environment, creation is done by the DMIh, under the responsibility of the head doctor, subject to the express condition that the hospital has checked the patient's identity via the Carenet platform. The local administrator oversees such authorisations, and a patient may contact him should he require any information or have any questions.
- A patient may also create his own access authorisations via www.rsw.be using his electronic ID card.
- Patients may also contact the RSW administration whose administrators are also in a position to carry out the requested actions.

Access authorisations expire automatically after a certain period of time (defined for each type of access authorisation). Patients may also revoke them beforehand.

There is a function available on the RSW enabling patients to view their access authorisations. This function is accessible to patients, to health professionals at the request of a patient (and requiring the right to access his records), to RSW administrators and to local administrators.

Levels of access rights

For each RSW function, one of the following levels can be assigned:

- 4 = Delete (automatically allows the edit / create / view functions)
- 3 = Modify (automatically allows the create / view functions)
- 2 = Create (automatically allows the view function)
- 1 = View (allows the read / download / print functions)
- 0 = None (access prohibited = default value for all users)

These rights may possibly be associated with restrictions.

User profile management

User rights are assigned via a user profile allocated to each user. A user profile unites people playing the same role within the system, and these people have access to the same list of functions within the RSW.

The RSW currently supports the following profiles:

- Administrators
- IT administrators
- Local administrators
- Patients
- Doctors
- RSW vouching doctors

Last update: 01/03/2013
In a later phase, further profiles will be added - for example
• Physiotherapists
• Nurses
• Pharmacists
• Other professionals in the sense of Royal Decree No. 78 of 10 November 1967 relating to the exercise of healthcare professions.

The full list of user profiles is to be found in the annex on the description of all access authorisations.

A user may possibly belong to several profiles.
The RSW administration is responsible for assigning user profiles to each individual.

The full list of which access rights are assigned is to be found in the annex. The table below lists, by way of example, the limited access rights of the initial RSW users. Patient access to their medical records is restricted in 2013 to persons involved in a pilot project and having given their explicit consent. The aim of this project is to define the practical modalities of such access in consultation with the public health authorities (SPF Santé Publique).
Assignment of access rights

The rights to access RSW functions are assigned to user profiles by the RSW administrators in accordance with a table such as follows:

<table>
<thead>
<tr>
<th>Function within the RSW</th>
<th>Patient</th>
<th>Doctor</th>
<th>RSW administrator</th>
<th>Local administrator</th>
<th>Vouching doctor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Patient registration and declaration of consent</td>
<td>4 F</td>
<td>4 D A</td>
<td>4 M</td>
<td>4 D A</td>
<td>0</td>
</tr>
<tr>
<td>Health professional registration</td>
<td>0</td>
<td>4 I</td>
<td>4 M</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Vouching for a health professional</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>4</td>
</tr>
<tr>
<td>Registering a user</td>
<td>0</td>
<td>0</td>
<td>4</td>
<td>4 P</td>
<td>0</td>
</tr>
<tr>
<td>Access authorisations</td>
<td>4 F</td>
<td>4 C</td>
<td>4 M</td>
<td>4 P</td>
<td>0</td>
</tr>
<tr>
<td>Making a medical record available on the RSW</td>
<td>0</td>
<td>4 I</td>
<td>0</td>
<td>4 P</td>
<td>0</td>
</tr>
<tr>
<td>Storing a medical record</td>
<td>0</td>
<td>4 I</td>
<td>4 M</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Deleting a medical record</td>
<td>0 F</td>
<td>4 I</td>
<td>4 M</td>
<td>4 P</td>
<td>0</td>
</tr>
<tr>
<td>Viewing the index of medical records</td>
<td>1 F</td>
<td>1 A</td>
<td>1 M</td>
<td>1 P</td>
<td>0</td>
</tr>
<tr>
<td>Viewing medical results</td>
<td>0 (1*)</td>
<td>1 A</td>
<td>1 M</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Viewing medical reports (non-psychiatric/non-genetic)</td>
<td>0 (1*)</td>
<td>1 A S</td>
<td>1 M</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Viewing psychogenic reports</td>
<td>0 (1*)</td>
<td>1 A S</td>
<td>1 M</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Viewing genetics reports</td>
<td>0 (1*)</td>
<td>1 A S</td>
<td>1 M</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Viewing the emergency health record (&quot;Sumehr&quot;)</td>
<td>0 (1*)</td>
<td>1 A</td>
<td>1 M</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Managing notifications</td>
<td>0</td>
<td>4 I</td>
<td>4 M</td>
<td>4 P</td>
<td>0</td>
</tr>
<tr>
<td>Restricting access to a given document</td>
<td>4 F</td>
<td>4 D A</td>
<td>4 M</td>
<td>4 P</td>
<td>0</td>
</tr>
<tr>
<td>Restricting the access of a health professional</td>
<td>4 F</td>
<td>4 D A</td>
<td>4 M</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Viewing the general access log</td>
<td>1 F</td>
<td>1 D A</td>
<td>1 M</td>
<td>1 P</td>
<td>0</td>
</tr>
<tr>
<td>Viewing the detailed access log</td>
<td>1 F</td>
<td>1 D A</td>
<td>1 M</td>
<td>1 P</td>
<td>0</td>
</tr>
<tr>
<td>Managing user profiles</td>
<td>0</td>
<td>0</td>
<td>4</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Allocating rights</td>
<td>0</td>
<td>0</td>
<td>4</td>
<td>4 P</td>
<td>0</td>
</tr>
</tbody>
</table>

The following restrictions are available:
- F = This function is limited to the person himself and to persons for whom he is the legal representative
- 1 = This function is limited to the person himself (his own personal records or records which he has produced)
- A = This function is dependent on the existence of an access authorisation
- S = This function is dependent on belonging to a specific medical discipline
- D = This function is to be done at a patient's request
- C = This function is dependent on the patient's electronic ID card (or that of his legal representative) being read
- P = This function is limited to data associated with a decentralised location
- N = This function is dependent on an explicit mandate from the person concerned
- * Accessed limited to volunteer patients in the context of the pilot project

Levels of access rights

- 4 = Delete (automatically allows the edit / create / view functions)
- 3 = Modify (automatically allows the create / view functions)
- 2 = Create (automatically allows the view function)
- 1 = View (allows the read / download / print functions)
- 0 = None (access prohibited _ default value for all users)

These rights may possibly be associated with restrictions.
**Access logging**

Any action carried out via the RSW is logged, whether it involves accessing centrally stored data on the RSW server or being exchanged via the network.

Log data must include:
- The type of action
- The action's timestamp
- The ID of the online user
- The patient ID
- The record ID (where applicable)
- The result of the assessment of the rights assigned to the user for the requested operation
- The status of the result of the action

**Viewing the general access log**
This involves viewing the list of health professionals who have accessed a patient's records. For each professional, one can see on which days an access was logged.

**Viewing the detailed access log**
This is a detailed list of all accesses to all of a patient's records. For each access, the following are listed: ID of the person online, the access timestamp (date/hour/minute/second), the institution from where the request came from (where applicable), the ID of the record consulted.
**Simplified example of how access to a medical result by a doctor is controlled**

Has the patient explicitly given his consent to the RSW Regulations?  
Yes → Has the doctor explicitly given his consent to the RSW Regulations?  
Yes → Does access authorisation exist for the doctor with regard to the patient in question?  
Yes → Control via his belonging to the doctor profile  
No → The doctor has the right to view medical results?  
Yes → The record has been declared relevant for exchange by its author?  
Yes → Is there any specific prohibition preventing the doctor accessing the result in question?  
Yes → The record is technically accessible  
No → The doctor will only view records relevant to the ongoing treatment of the patient he is treating  
No → The access is logged  
Yes → The doctor is bound to professional secrecy  
No →
§8. Data security

It should be noted at this juncture that, when properly designed, the security of computerised medical records is much better than that of paper records. Given its uniqueness, the destruction (e.g. by fire) or loss of a paper file is often irreversible. In addition, the viewing of a paper file is not logged. Using computerised records, one can keep back-up copies at remote locations and log all accesses.

The Security Consultant is there to ensure that FRATEM implements all realistic means to ensure a state-of-the-art level of security of RSW data in accordance with legal provisions.

The RSW security policy describes the security principles and how these are implemented. The complete security policy is to be reviewed every two years.

Similarly an audit of each security perimeter is to be conducted at least once every two years.

We would like to remind readers that the intention of the system is to improve the dissemination of medical records, while ensuring that all accesses to health data are legitimate. This is no substitute for the legal requirements regarding information storage in secure local systems (DMIh and DMIg). Instead the RSW system is to be seen as complementing these storage systems through facilitating the exchange of the stored data.
§9. Glossary (in the sense of the RSW)

Accreditation (within the RSW)
Accreditation is the recognition of health professionals authorised to exchange medical records within the RSW.

Anonymisation
A process making data not assignable to an identifiable person. It is used in the context of scientific and epidemiological studies.

Access authorisation (within the RSW)
This is a right assigned to a health professional (accredited by the RSW) to access administrative or medical records according to context-specific criteria (e.g.: the existence of a therapeutic link in order to be able to process the data of a given patient)

Authenticity
Property ensuring that the identity of a subject or a resource is actually that declared. Authenticity applies to such entities as users, processes, systems and information.

Authentification
Process for ensuring the authenticity of a person, entity, process, system or information.

Directory
List of persons constituting a catalogue containing certain administrative details
Example: Patient directory (list of patients registered with the RSW, containing their names, forenames, regional ID numbers).

Confidentiality
Property of a piece of information to not be available or not to be disclosed to any non-authorised individual, entity or process.

Conformity
Character of a product, process or service meeting all set requirements.

Consent of the person concerned
By "consent of the person concerned" we understand any specific and informed manifestation of free will, through which the person concerned or his legal representative accepts that personal data concerning his person may be processed

Approved DMI system
Software system used for managing computerised medical records and which has been audited with a view to guaranteeing its functional compatibility with the RSW (the French term DMI - dossiers médicaux informatisés - is used in this document)

Medical record
Any structured record of consistent health data.
Examples: lab results, a X-ray image.

Centralised data
Patient data stored on the RSW server (a patient's identification data, active therapeutic links, positive and negative authorisations to access patient data, index of stored records, access logs)

Access rights (powers or privileges)
Technical mechanisms within the system governing accesses in accordance with assigned authorisations.

Certification (FR: Homologation)
The authorisation to use, for a specific purpose or under specific conditions, a product or a system Certification is done by the RSW, in accordance with pre-defined criteria.

Identifier
The technical code allowing an entity to be identified
**Identification**
Process involving the communication of one's identity to an entity (person, process, system).

**Identity**
Symbolic information allowing the unique designation of an entity (e.g.: a name, a pseudonym, a code)

**Therapeutic link to a patient**
Relation between a given patient and a health professional bound to professional secrecy and personally involved in the ongoing treatment of the patient (diagnosis, treatment or prevention).

**Orbac (organisation-based access control)**
Principle of controlling access to computerised data in accordance with the user's role and activity.

**Patient**
The subject of the medical records transferred.

**Trusted person**
At the request of a patient, data may be communicated to a trusted person he has designated.

**Health professional**
A healthcare professional as defined in Royal Decree No. 78 of 10 November 1967 on the exercise of healthcare professions. Examples: general practitioners (GPs), radiologists, nurses

**Legal representative**
When the patient is a minor, he is represented by a parent (father or mother) or the legal guardian. Doctors may however decide, on account of the age and maturity of the patient, to bring the latter into the system.

If the patient is an adult but has prolonged minority status, his patient rights are then exercised by the parent or legal guardian. The doctor may however deem it opportune to bring the patient into the system, dependent on his level of comprehension.

If the patient is an adult and has no prolonged minority status and if the patient has designated a legal representative in advance, the latter may act on his behalf insofar as and for the period of time in which he unable to personally exercise his rights (subject to the doctor's judgment). By default, a patient's rights may be exercised by his spouse (not when estranged) and by his common-law partner. By default, and insofar as there is no conflict between the parties concerned, the rights can be exercised by an adult child, a parent, or an adult brother or sister. By default (or in the case of a conflict), patient rights may be exercised by the GP, possibly supported by a multidisciplinary commission overseeing the patient's interests.

In all cases, when a GP deems that a request from a legal representative to view or obtain a copy of a patient's records can be harmful to a patient's interests, he may refuse all or part thereof. In such a case, the right to view is exercised by the GP designated by the legal representative.

**Processing entity (FR: Responsible du traitement)**
The physical person or legal entity, association or public authority which, alone or in conjunction with others, determines the purposes and means of processing personal data.

**Subcontractor**
The physical person or legal entity, association or public authority processing the personal data on behalf of the processing entity and who is other than the person who, placed under the direct authority of the processing entity, is authorised to process the data.

**Sumehr**
The "summarised electronic health record" of a patient, corresponding to a "snapshot" of a patient's health and taken by the treating doctor in his capacity as manager of the patient's overall medical file (Dossier Médical Global or DMG) in the context of his privileged contacts with the patient. Far from being static, the sumehr evolves over time in line with the patient's medical history. It is not a complete medical file but only an extract thereof, containing data useful for follow-up treatment.