Centre de Ressources des Technologies pour la Santé

# LABO - Work Package WP4 - Cahier des charges fonctionnel

Requirements Document

Guido Bosch
Version 1.0
9/1/2012

Centre de Ressources des Technologies pour la Santé

# CR SANTEC

| | | | |
|---|---|---|---|
| Project | LABO | | |
| Work Package | WP4 – Functional Require | | |
| Project Manager | | Stefan Benzschawel | stefan.benzschawel@tudor.lu |
| Author | | Guido Bosch | guido.bosch@tudor.lu |

# List of Dissemination

| Name | Organisation | Email | For validation | For comment | For info |
|---|---|---|---|---|---|
| René KRIPPES | Direction de la Santé | Rene.Krippes@ms.etat.lu | X | | |
| Jean-Charles Dron | Health Management Solutions | jcdron@hms-france.com | X | | |
| Dr. Claude Schummer | AMMD | schumcl@pt.lu | | X | |
| Dr. Jill Koullen | AMMD | drjk@pt.lu | | X | |
| Dr. Stefan Benzschawel | CRP Henri Tudor | Stefan.benzschawel@tudor.lu | | X | |
| Dr. Cédric Pruski | CRP Henri Tudor | cedric.pruski@tudor.lu | | X | |
| Claude Poupart | CRP Henri Tudor | claude.poupart@tudor.lu | | X | |
| Heiko Zimmermann | CRP Henri Tudor | heiko.zimmermann@tudor.lu | | X | |
| François Wisniewski | CRP Henri Tudor | Francois.wisniewski@tudor.lu | | X | |
| Serge Frieden | EHL | serge.frieden@ehl.lu | | X | |
| Pierre Gilbert | CHL | Gilbert.Pierre@chl.lu | | X | |
| Raphael Laschiazza | EHL | laschiazza@gmail.com | | X | |
| Christophe Nardin | EHL | christophe.nardin@ehl.lu | | X | |
| Laure Pellerin | EHL | laure.pellerin@ehl.lu | | X | |
| Patricia Borde | LNS | Patricia.Borde@lns.etat.lu | | X | |
| Georges Gilson | CHL | gilson.georges@chl.lu | | X | |
| Danielle Meunier | CHEM | mail@meunier.lu | | X | |
| Jean-Marc Michels | Zithaklinik | jean-marc.michels@zitha.lu | | X | |
| Jacqueline Parmentier | Hôpital Saint Louis | Jacqueline.Parmentier@chdn.lu | | X | |
| Pol Brouart | FFE | pol.brouart@ffe.lu | | X | |
| Annick Martin | FFE | annick.martin@ffe.lu | | X | |
| Paul Courrier | Croix-Rouge | paul.courrier@croix-rouge.lu | | X | |
| Patrick Brochot | Ketterthil, / FLLAM | patrick.brochot@ketterthill.lu | | X | |
| Jean-Luc Dourson | Ketterthill / FLLAM | jean-luc.dourson@ketterthill.lu | | X | |
| Patrick Njiwoua | INFOMED/ Ketterthill | patrick.njiwoua@ketterthill.lu | | X | |
| Manfred Pichler | Laboratoires Réunis | pim@labo.lu | | X | |

## Goal of the Document

This document describes the activities that the eSanté system must perform to achieve its desired outputs; that is, which transformations are necessary to turn the available inputs into the desired outputs. More specifically it describes what the system is supposed to do when exchanging, i.e. submitting and consuming lab reports over the platform.

It represents a requirements document at the functional level, which is an essential part in the requirements analysis process. Only when the major stakeholders agree on the functional specification in this document the analysis should advance to the more detailed technical level.

## State of the Document

The information contained in this document reflects the status of an ongoing discussion within the LABO project, especially in the Labo workgroup (GT Labo). Final approval has been obtained for version 0.6 by all major stakeholders, on 23/12/2011.

The document is published in its final version 1.0.

## Change History

| Version | Date | Author | Modification |
|---|---|---|---|
| 0.1 | 26/9/2011 | GBO | Initial draft |
| 0.2 | 14/10/2011 | GBO | • XDR recipients and XDS viewers are to be notified of cancelations. The labo gets the list of all actual readers, both XDS and XDR.<br>• Patients can see the last of a series of reports, be it partial or complete. |
| 0.3 | 14/11/2011 | GBO | SubmitLaboratoryReportXDS: There is no more APND linking between lab reports. Replacement (RPLC-linking) becomes the prevailing mechanism in the submission of successive lab reports. We also dropped type limitations for replacement documents in ReplaceDocumentXDS & ReplaceDocumentXDR. As a consequence sequences of chained reports do no longer occur in the mockup screens, even for doctors. With replacement there exists only one current version at a given time. |
| 0.4 | 30/11/2011 | GBO | Integration of RK's remarks.<br>Documentation for parameter 'Abnormal results' added were missing. Two new sections in Chapter §5: "Replacing vs. Appending Lab Reports" and "Patient Read Blocking Flag and Unblocking Code". |
| 0.5 | 8/12/2011 | GBO | Some changes in §5 "Patient Read Blocking Flag and Unblocking Code" and in the Glossary of terms. |
| 0.6 | 9/12/2011 | GBO | Improvement of formatting, especially page breaks. |
| 1.0 | 9/1/20112 | GBO | Final version after approval - no changes since 0.6. |

# Table of Contents

# §1 Method and Terminology

A functional requirements document defines the functions of a software system and its components. A function is described as a set of inputs, the behavior, and outputs.
In contrast to the Use Cases, which are descriptions of the interactions between the users and the system, the functional requirements are described in terms of calculations, technical details, data manipulation, data processing and other specific functionality that defines what the system is supposed to accomplish. Therefore functional requirements focus on particular results of a system and its components.

Functional requirements are supported by non-functional requirements, which impose constraints on the design or implementation (such as requirements about security, performance or reliability). Those are not covered in the present document, as they belong to the scope of the core platform requirements, not to the LABO specific part.

Depending on where the functions will be used we use different methods for their description. The data provider functions are mainly, though not exclusively, used in larger institutions like hospitals and laboratories, where they will interface with existing information systems such as HIS, LIS or Enterprise Application Interfaces (EAI). They are specified in a rather sober, technical style by means of ***Transactions***, which are technically precise and destined to a more technically trained readership such as IT personnel.

> **Transactions** are interactions between actors that communicate information through messages. If a transaction succeeds a result is returned, and all its processing side effects become visible (***committed***) to the rest of the system. This also means that during the transaction the intermediate processing results remain invisible to other participants of the system. If a transaction fails it is ***rolled back***, meaning that all of its processing effects are undone, and the system is left in the same state as if the transaction would have never been invoked in the first place, with the exception of log entries.
> Transactions also return ***results*** if they succeed or a ***failure message*** if they fail.
> The exact technical means for returning results, both positive and negative, is not detailed here (black box). It is more important to mention that a transaction runs synchronously, meaning that the calling system has to wait for the return of a transaction's result before being able to send the next transaction.

The data querying, retrieving and viewer functions of the eSanté system are mainly, although not exclusively, used by HCPs, such as general physicians, medical specialists and para-medical professionals, and of course the patients. This typically constitutes a group of users of non-IT-experts, and validation of formal transactional specifications could prove difficult to the majority of them. We therefore opt to describe these functions in a rather informal, textual way, illustrated by so called ***mock-up screens*** that provide the user with a visual impression of the function's working.

> **Mock-up screens:** In software development the most common use of mock-ups in is to create fictitious user interfaces that demonstrate what the software will do. Mock-ups can range from very simple hand drawn screen layouts, through realistic bitmaps, to semi functional user interfaces developed in a software development tool.

In this case we have opted for simple drawings of screen GUIs, with sample data to provide content and material for discussion. The real functional specification is given by the text that

surrounds the mock-ups. We would also like to stress here that those mock-ups do not represent an actual graphical specification for the GUI layout of the future eSanté Web Viewer software, but merely serve as illustrations for the functionality that this Web Viewer will provide. It is much more likely that, instead of the classical GUI mock-up screens used in this document the eSanté Web Viewer will be designed with a modern, multi-tabbed Web browser interface in mind.

A glossary which defines the meaning of specific terms is added at the end of the document. Hyperlinks into the glossary are provided throughout the text whenever appropriate. Use Crl-Left-MouseClick to jump to the definition in the glossary. Type Alt-← (left arrow) to jump back.

If you view the document with MS-Word consider to activate Bookmark visibility (Word Options → Advanced → Show document content → Show Bookmarks). With the bookmarks highlighted in the text it becomes easier to use them for navigation.

# §2 Architectural Considerations

The eSanté platform is a complex system made of several layers of components and protocols to communicate between those layers. The protocol chosen to talk to eSanté, and thus the level of available functionality, depends on the component layer that is addressed. Although it is not the goal of this document to specify those different layers in detail, they need to be introduced so that the reader can understand which level of functionality can be expected from which component level. Especially the components called ***Connector*** form a distinguishable layer around the so-called ***eSanté Core System***. Broadly speaking, Connectors are components that sit between the Core System and the Data Providers / Consumers.

Figure 1 depicts the communication level that is described by the functional specifications contained in this document, in respect with the Core System functionality.

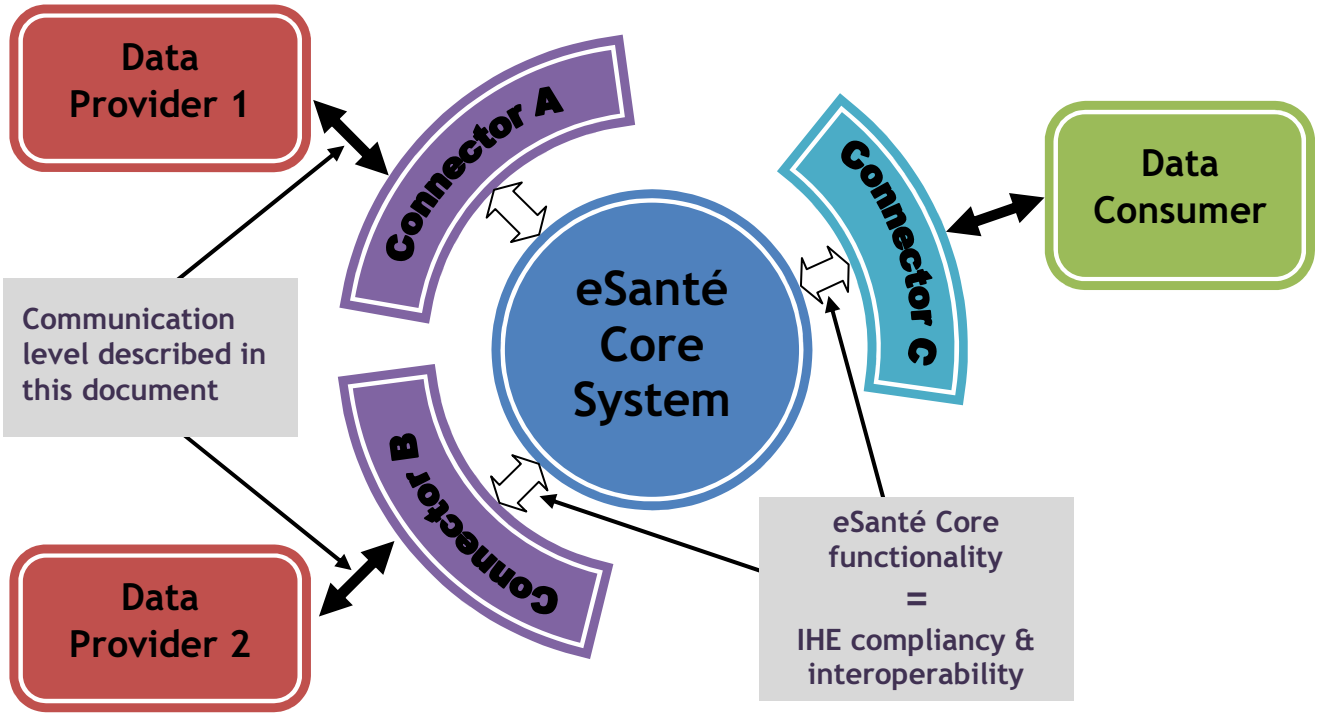



**Figure 1: Communication levels between Providers/Consumers, Connectors and the eSanté Core System**

It shows that the Data Providers talk to eSanté not directly, but through the connectors. The present document describes the functional layer offered by the connectors, not the ones of the Core System. This means that

a) the providers/consumers talk the "connector language", not the core language

b) the connectors implement additional functionality in respect with the eSanté Core

The need for connectors has two main causes:

1) The Core System will conform as much as possible to the IHE profile specifications and their protocols in order to become interoperable to other IHE compliant systems. This seems reasonable because being aligned to emerging international standards promises cost reduction through improved interoperability, if the vendors are conforming to those standards. Nevertheless, as the Core System is very generic in its functionalities, it leaves

a lot of the specific eSanté functionality to be implemented in the connected systems (Providers & Consumers), such as patient de-identification, document signature, encryption etc. An additional implementation effort will therefore be required by all connected actors, which could be reduced by developing a connector component that already implements the common behavior.

2) As two recent studies involving Luxemburgish hospitals and laboratories have shown, the existing Data Providers fulfill IHE interoperability requirements only to a very small degree. It would require large efforts for them to become interoperable with the eSanté Core, which has opted for a strong IHE compliance. A simpler and easier target to reach is therefore a level of communication and functionality that is closer to the connected systems, such as i.e. transactions based on HL7 messages for providers, and specific Web services and APIs for consumers.

However, the use of a connector to communicate with eSanté is not the only possible choice for a connected system, as Figure 2 shows.

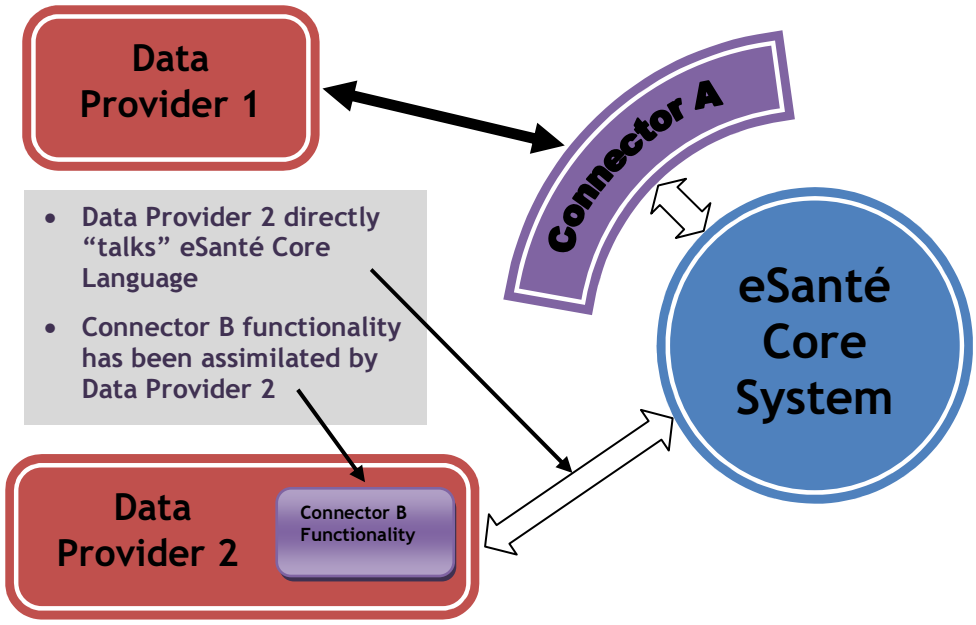



Figure 2: Direct Connection of a Data Provider to the eSanté Core Platform

Depending on the (future) level of IHE interoperability of available health care software and the effort that can be spent by the external actors to implement the required business logic in their core systems (LIS, HIS/RIS/PACS, PMS etc.), a direct eSanté core interoperability remains a viable alternative. Actually, this should be the preferred choice for new developments, but right now the connector serves as a "functional buffer" that allows to be more flexible and cost-effective when connecting existing systems to the eSanté platform.

By introducing the intermediate Connector component, the suggested architecture will keep the eSanté core open for general IHE interoperability, and at the same time allow the connected actors to have a functional buffer between eSanté and their own systems, which often cannot be changed so easily and quickly, and with reasonable effort and cost. It also sets a clear target for those systems if they want to achieve better, standardized interoperability, not only with eSanté, but also with other IHE compliant actors inside and outside of Luxemburg. The distinction between core and connector functionalities is made explicit in [LABO WP5 CDC Technique].

# §3 Overall Framework for Data Transmission and Sharing

The eSanté platform provides the general framework for data sharing and transmission of laboratory test data. There are two basic goals that this platform has to achieve:

1. The platform must guarantee the secure delivery of medical data to all HCPs who have been designated to receive it.
2. The platform should build, over time, a secure record of medical data for identifiable, participating patients, and allow those data to be shared with and managed by HCPs that are involved in those patients' health care.

The first goal requires that the recipients of the data are uniquely identified so that delivery can happen. The second goal requires that patients can be uniquely identified and are willing to share their medical data with other participants, so that a Shared Patient Health Record (SPHR) can be built for them. Figure 3 shows how the eSanté platform puts these goals into practice.

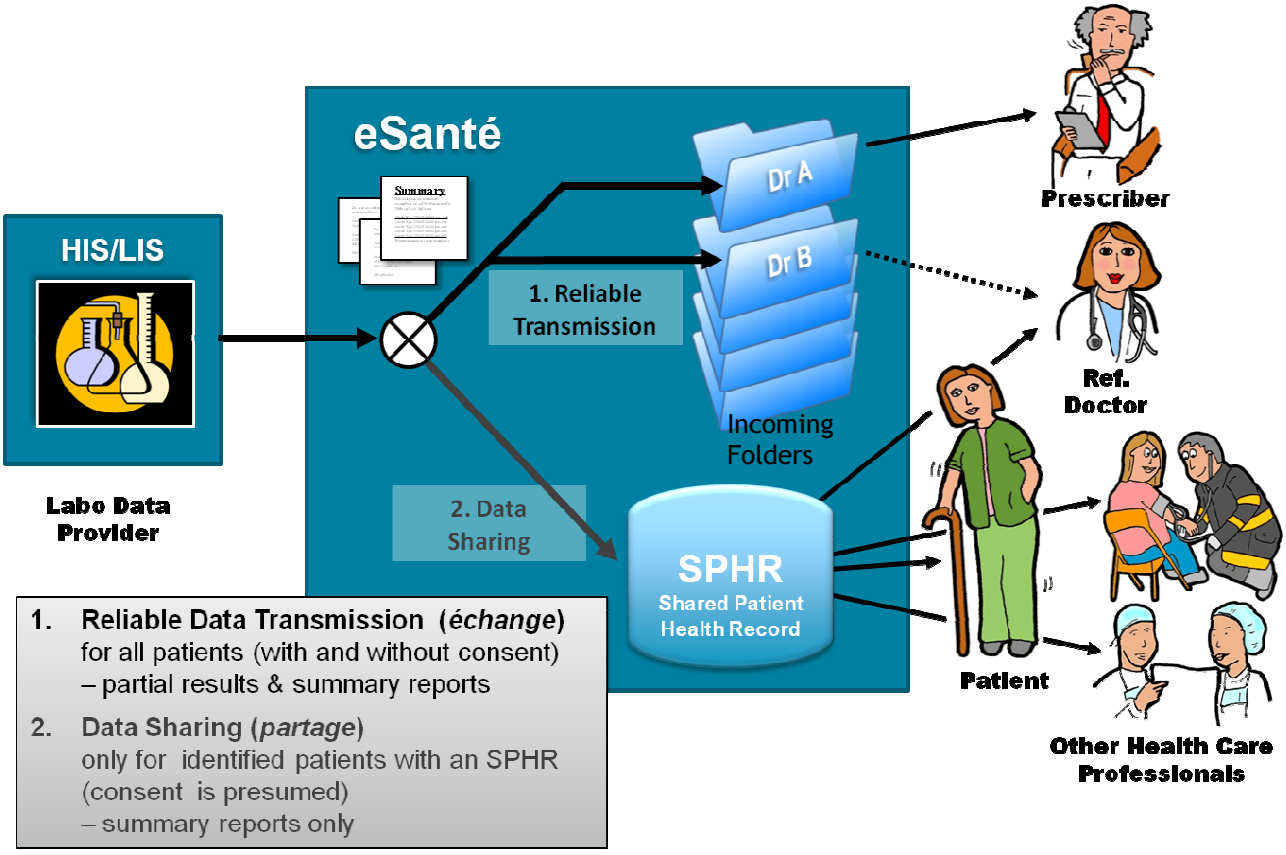



Figure 3: Overall Data Exchange in eSanté

Depending on the patient situation and the information known during data submission only one or both goals can be achieved. The patient's consent situation, his statute in the Luxemburgish health system, as well as identification issues determine which goals can be met. More specifically a patient's medical data may

- **transit over the platform** («*service d'échange*»), i.e. it will be delivered directly to the recipients such as the prescriber, the reference doctor, specialist etc. This is done by placing it into the so called Incoming Folder, a private storage area for every participating HCP. Once

downloaded from there the data will no longer reside on the platform[1]. This transmission is possible whenever one or more recipients are provided, even for patients who have not given or revoked their consent, or are not enrolled at all in the Luxemburgish health system, or simply because they couldn't be uniquely identified by the system. Because this works for all situations as long as the recipients are known we also refer to it as **Reliable Transmission** («*service d'échange*»).

- be **permanently stored on the eSanté platform**, in his SPHR if he has been identified, and if he has a positive consent situation. This is also referred to as **Data Sharing** («*service de partage*»). It is this part of the eSanté platform that adds a lot of value to the patient's health care, because it allows the implementation of useful functions such as easy data sharing among health professionals, centralized management of a patient's health record by a reference doctor, direct patient access to his own health record, patient referral, electronic prescriptions, etc.

It should be noted that, depending on his roles and privileges, the same health care professional can have access to a patient's data via both access methods: The reference doctor e.g. may have a permanent access to his patients SPHR while also receiving copies of all new results for exams he prescribed, but the access modalities and viewpoints will be different:

- The **Reliable Transmission** delivers individual documents (such as lab test reports) to an identified receiver (prescriber, reference doctor, ...) for all his patients. In reference to the corresponding IHE profile we also use the abbreviation XDR to denominate this case.
- The **Data Sharing** over the SPHR shows both new and historical documents for one selected patient at a time (XDS in IHE terminology)

eSanté stores submitted documents in two separate structures called Document Registry and Document Repository. The registry holds the document's metadata and a link to the document's content, which is stored in the repository, and to the patient in the Patient Registry.

The metadata will be used for displaying document summary lines, to locate the content, and serve as search criteria for document queries. The set of documents referring to the same patient thereby forms a so called longitudinal record, in other words the SPHR.

Figure 4 shows an example of the pair "Document Registry" and "Repository" with two longitudinal records: patient X with lab reports A, B & E and patient Y with radiology documents C & D.

[1] Except for log entries. The documents however will be deleted.

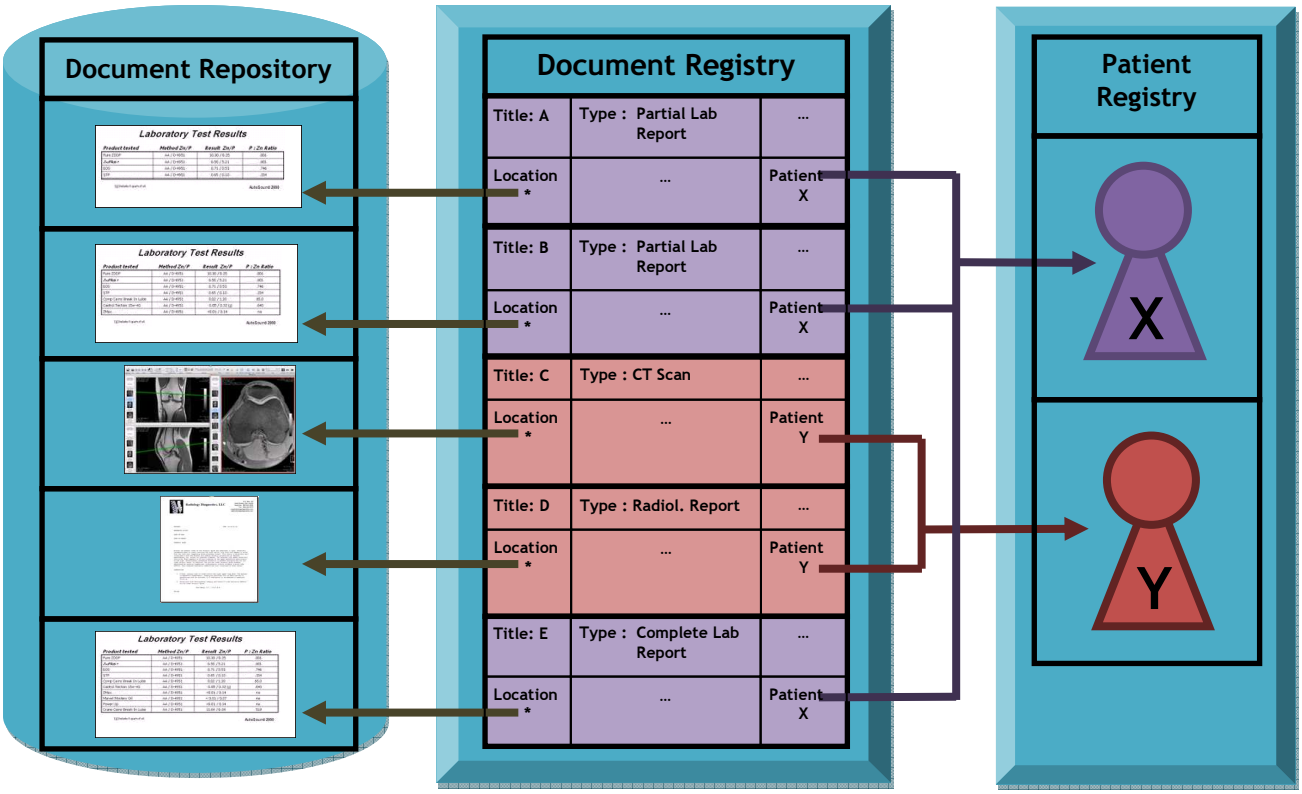



**Figure 4: Example of Longitudinal Patient Health Records**

# §4 Summary of the LABO Use Cases

This Chapter briefly summarizes the major results of the LABO Use Case specification (LABO-WP2-UseCases-2.0.pdf) in order to recall the context of the eSanté LABO data exchange and its different functions.

- **LAB-UC1: Labo Data Provider**
  The labs send, through their existing LIS, clinically validated lab test reports in form of standardised XML documents (CDA) to the eSanté platform, where they are stored in the patient's longitudinal record. Additionally the reports are transmitted directly into the Incoming Folders of the prescriber and other identified recipients.
  Test reports originating from the same prescription can be sent in several stages of completeness at different times: partial reports contain only a subset of the ordered results and are thus incomplete. Subsequent partial reports contain more and more results, until the last complete report is sent, which contains all the ordered results, Although all complete reports are in principle available for the patient, some may exceptionally be blocked from patient viewing if the prescriber has explicitly asked for it.
- **LAB-UC2: Lab Result Cancellation & Replacement**
  If errors occur in a lab report, or in its transmission, the issuing lab can cancel the report and possibly replace it with a newer, corrected version. Cancellation in combination with resubmission can be used to correct the wrong transmission of an otherwise correct report (report associated with the wrong patient, or sent to the wrong HCP).
  Cancellation messages are delivered into the recipients Incoming Folders if they have already downloaded the document, otherwise the document is canceled or replaced "silently". Email notifications are sent to everybody who has explicitly subscribed to such a type of event (see LAB-UC6 below).
  The canceling lab gets the list of all recipients and XDS viewers who have already downloaded and seen the report so that it can take additional measures to inform his customers.
- **LAB-UC3 Single Patient Data Viewing & Import**
  Reference doctors and other authorized HCPs view lab test results in the SPHR of one single patient. Prescribers and other HCPs can access all reports, partial and complete (patients see only the last report in a series, i.e. the most recent one).
  Abnormal values in a report may be highlighted for HCPs, while patients can see only the raw, uninterpreted values. Nevertheless, these are display variations of the same report, not different documents. The same holds for individual display styles that a lab may define for viewing its own reports.
  If a report was blocked for patient viewing by the Data Provider, the HCP can unblock it.
  Optionally the viewer can download and store the document on its own computer for later off-line visualization and PMS-filing.
- **LAB-UC4: Patient Data Viewing**
  The patient can view and possibly download his own complete lab reports. If they are blocked for patient viewing he may unblock them if he has been given the correct unblocking code.
  When viewing a report for the first time the viewer software should display a message inciting the patient to seek the council of a qualified HCP to interpret the results for him.
- **LAB-UC5: Reliable Data Transmission**
  HCPs who are the recipients of lab reports (and other types of documents) download them directly from their Incoming Folder on the eSanté platform. Once downloaded and

decrypted locally they are removed from the folder on the platform. The HCP can now visualization the documents off-line and file them in his own PMS.

- **LAB-UC6: Notification Subscription / Unsubscriptio**
  Patients, doctors and in general any person participating in the eSanté platform can subscribe to be notified when certain events occur such as the arrival of new laboratory results or the cancelling / replacement of existing ones.

# §5 Data Submission Transactions

As explained in Chapter §2 -Architectural Considerations, the scope of the current functional specification includes the connector component level, whereas the core platform is limited to IHE compliant specifications. As a consequence the data submission transactions specified in this chapter are not identical to the IHE transaction "*Provide and Register Document Set-b [ITI-41]*", although somewhat inspired by it. E.g., there is only one ITI-41 transaction for all kinds of data submission, whereas we define separate transactions for each transmission path that is appropriate (XDS, XDR). This breaks down the specification into simpler functional units, and also creates simpler situations for dealing with failures and exceptions. Similarities with ITI-41 are the existence of a metadata segment for the whole transmission set, and the use of the HL7-CDA R2 format for all submitted documents.

There is also a non-data-transmission transaction in this Chapter, CancelDocument, which has no XDS/XDR flavor. It doesn't deal with data submission, but rather with document state changes and removal of documents.

### *Formalism to describe transactions*

We need to stress that, for the purpose of presenting precise specifications some formal framework for describing transactions has to be used. Especially the input parameters of the transactions have to be named, typed and specified to a certain degree. However, this does not preclude any modifications to details that may become apparent and necessary during later stages of the project. Here again one can see that the connector layer acts as a safeguard to ensure the translation between the eSanté core platform language and the more flexible functional specification level introduced by this document.

The description of a transaction in this document follows this structure:

**Input:** List of input parameters, their cardinality (0, 1 or more) and their types. The input data consist of

- **metadata** for the whole transaction which may contain, among other, identification information for a patient, the Data Provider and the Data Recipients.
- **a document** or a **document reference** to an already submitted document. Documents represent new data to submit, and come with their own, non-encrypted metadata[2], which will allow for queries to search, filter and order, and also to create summary lines in different views. References on the other hand allow to refer to previously submitted documents, e.g. to connect them with new documents such as the successive partial reports and the complete report, or to replace or cancel them.

**Validation:** Control of the parameters to check their validity. If any part of the validation fails the processing is skipped and the transaction is aborted, i.e. output = 'Failure'.

**Processing:** The main execution performed by the transaction. If the conditions for a complete and correct processing are not met, or an unrecoverable error occurs, the processing fails, and with it the whole transaction (output = 'Failure').

[2] Document content must be encrypted before it is sent to eSanté, where it is stored in the Document Repository, while metadata are transferred and stored readably in the Registry. The exact mechanism, the so-called Re-Key Encryption, is explained in the "LABO CDC technique" (technical specifications) and in Chapter 5 of the document "Architecture and Security of a National eHealth Platform", version 1.26 of 29/6/2011.

**Output:** The result of a transaction. In most cases this is just 'Success' or 'Failure'. In the case of failure an error messages indicating the reason of the failure shall be returned. But it can also be any other type of information, such as the list of readers of a document in QueryDocumentReaders.

**Notes:** Additional notes and comments about the transaction.

Whenever appropriate the main points are broken into smaller fragments, which are numbered for easier reference.

### *Universally Unique IDs (UUIDs)*

The documents submitted in transactions and the transactions themselves are uniquely identified, at the provider's side, by so called **Universally Unique IDs** (UUIDs). They are the document references mentioned above. Because the Data Provider generates and puts them into his own documents he has always the means to refer uniquely to his documents. Data consumers will run queries against the Document Registry, and if there are matching entries the result should contain UUIDs for all matching documents. The consumer can then use these UUIDs to retrieve the documents from the Repository in a separate query.

Transactions also have their own UUIDs, generated by the Data Provider. They refer to complete transactions and will appear in transaction log files. They can be used e.g. in case of problems to track down a particular transaction.

### *Replacing vs. Appending Lab Reports*

[**IHE Lab TF-3 Vol3**] states in Section 2.2.1.3 DSDocumentEntry.parentDocumentRelationship, p. 8, that:

> 'XD-LAB only permits the "replace" relationship between instances of XD-LAB documents. Thus, XDSDocumentEntry.parentDocumentRelationship is constrained to only the "RPLC" value.'

This excludes the usage of 'APND' document links as a means to link together all reports that belong to the same prescription, and suggest the use of document replacement instead ('RPLC' links). As a replaced document is given the status 'deprecated', meaning: no longer accessible for regular Data Consumers, the consequence is that only the latest of a series of lab reports submitted for the same prescription will be visible to Data Consumers. Older versions will be deprecated and become invisible. This makes no difference for the patient, who should only see the latest, complete report, anyway. However, doctors who are looking into a patient's SPHR will, at any given time, only find one version of a lab report: the most recent one, which can be partial or complete.[3]

The transactions in this chapter have been designed with IHE's strict 'RPLC' policy in mind. However, we should consider this level of specification as an implementation detail and remain open to an 'APND' based solutions as well.

### *Patient Read Blocking Flag and Unblocking Code*

The XDS transactions that submit documents (SubmitLaboratoryReportXDS, ReplaceDocumentXDS) carry two optional parameters, **Patient Read Blocking** and **Unblocking Code.** The first specifies if the patient is not allowed to read a document, and in this case the second parameter should provide a code that the doctor can give to the patient so that he can unblock it himself.

[3] This is not true for XDR transmitted reports, which are sent as unlinked documents, which can always be downloaded from the recipients' Incoming Folder, even if a newer report has already arrived.

Both the read blocking flag and the unblocking code should also appear in the document's metadata[4]. Furthermore, the reports that are distributed by the lab directly to the doctors (printed paper version, on-line report etc.) should also display the unblocking code, if present.

There are several reasons why those two parameters have to be present at the transaction level:

- A Data Provider receives a digitally signed report from a third party and wants to send it to eSanté without compromising the integrity of the original document. Nevertheless, the third party's settings for those metadata are not existing, or inappropriate. By using the corresponding transaction parameters the Data Provider can now override the settings in the document without changing the original report.
- A similar situation occurs if the Data Provider uses digitally signed CDA documents internally, and their transmission to eSanté is only a secondary usage.
- There are documents that could benefit from the blocking/unblocking features which are not available in a HL7 CDA format, and therefore may not be able to store the required metadata (example: DICOM KOS files)[5]. The transaction parameters are a good mechanism to send this information, anyway.

As those attributes can now be present in two different places (transaction and submitted document), rules have to be defined in case when the values are different.

**Patient Read Blocking**
The following table shows the different combinations that are possible, and their resolution.

| Patient Read Blocking | | |
|---|---|---|
| **In parameter** | **In document** | **Meaning** |
| **No** | No/not present | Document not blocked for patient reading |
| **No** | Yes | Document not blocked for patient reading |
| **Yes** | No/not present | Document blocked for patient reading |
| **Yes** | Yes | Document blocked for patient reading |

As one can see, the parameter's value overrides the one in the document. This is also true if the read blocking flag is not present in the document at all. If the flag is missing in both the document and the optional transaction parameter, then the default value specified in the transaction applies.

**Unblocking Code**
If a document is blocked for patient reading, the Data Provider should also generate an unblocking code and put it into the document and the submission transaction. In this normal case there is no discrepancy between the document metadata and the transaction. However, for the above mentioned reasons there can be differences, and here is how they are resolved:

[4] There is a "confidentialitycode" in the standard CDA metadata specification that will be used to hold the information corresponding to the read blocking flag.
[5] Although DICOM KOS is not relevant for the LABO scenarios, please keep in mind that the patient read blocking/unblocking feature can be useful for all kinds of clinical documents.

| Unblocking Code present | | |
|---|---|---|
| **In parameter** | **In document** | **Meaning** |
| — | — | The patient cannot unblock the document. It can only be unblocked by an authorized HCP.[6] |
| Present | — | Patient unblocking possible with the code given in the parameter. |
| — | Present | Combination not allowed. If the code is in the document it must also be present in the parameter. If not, the transaction fails. |
| Present | Present | Patient unblocking is possible, if both codes are equal. If not the transaction fails with an appropriate error message.<br>This avoids having an unblocking code in the document that would not work. |

## §5.1 Transaction: SubmitLaboratoryReportXDR

This Transaction handles the principal document submissions for the Reliable Transmission scenario (XDR), by sending one lab test report to one or more identified recipients.

### Input

| | | |
|---|---|---|
| Transaction ID | 1 | UUID |
| Recipient Identification Info | 1 or more | see glossary entry |
| Provider Identification | 1 | see glossary entry |
| Title | 0 or 1 | Text |
| Comments | 0 or 1 | Text |
| Lab Report | 1 | Structured or unstructured report |
| Abnormal Results | 1 | Yes/No |

### Validation

1. **Recipient Identification info** for one or more receiving HCPs must be provided. Every single recipient must be resolved to a registered HCP,[7] otherwise the transaction fails (see also processing step 1).
2. **Provider Identification** is mandatory. The provider has to identify himself in every data submission, otherwise the transaction fails.
3. **Title and Comments** are optional texts that may be given to document the transaction itself. They can, but do not have to be identical to the **Lab Report**'s own title and comment in the document's header.
4. **Lab Report** is mandatory. Each transaction contains exactly one report, which may be a partial or a complete lab report.

[6] A blocked document can always be unblocked by an authorized HCP, even without unblocking code.
[7] How the Data Provider obtains the valid recipient identification is not specified in this document, and should be addressed elsewhere, because it is a common concern for all kinds of Data Providers in the whole eSanté system. A special "HCP directory service" could be imagined, that allows for individual HCP ID resolution and for synchronizing with a locally kept list of HCPs.

5. **Abnormal Results** is a flag that is be set by the Data Provider to signal the presence of abnormal or otherwise unusual test results, in order to alert the physician to give this report some priority. Default: No.
6. **Availability of Patient Identification Data in the documents**: The document provided in the transaction should contain in its content sufficient information that allows the reader to identify the patient to whom the document belongs, such as name, first name, birth date, matricule etc.[8] Only the presence of this information in the document is checked, not its semantic validity.

## Processing

1. The system uses the **Recipient Identification Info** to find a unique match for each recipient within the system's Health Care Professional Registry. If one of the recipients could not be uniquely identified the transaction fails with an explanatory error message such as "Recipients not found: <list of unidentified recipients>".
2. With all recipients positively identified the **Lab Report** is placed in every recipient's Incoming Folder from where they can download it.[9]
3. All recipients who have subscribed to the Notification Service for the arrival of new lab reports are notified by email.

## Output

If an irresolvable exceptional situation is encountered during **Validation** or **Processing,** then the status 'Failure', with an appropriate error message, is returned as the result of the transaction, otherwise the result is 'Success'.

When failure occurs all of the transaction's side effects described under Processing are rolled back, i.e. they actually do not happen at all.

## Notes

1. If the transaction fails for any number of reasons (input validation failed, processing failures, unavailability of system components, …) the whole transaction fails. This is an important principle in order to keep the eSanté platform free of incomplete or partially executed data submissions, which it would have to recover from later on. The error message returned at the failure point helps to diagnose the problem that led to the failure. The Data Provider can then try to submit the transaction again, possibly with a different input, but by doing so it remains his responsibility to submit a complete and coherent document with its metadata.
2. More specifically, the transaction fails if at least one recipient could not be identified, because the delivery of the documents could not be guaranteed in all cases. If a partially successful transmission was allowed this would require the implementation of partial failure feedback to the provider, and possibly complex retrial mechanisms to compensate for a bad recipient identification. It is therefore much simpler and reliable to accept only

[8] We do not specify which exact identification criteria have to be present, as this is still an ongoing discussion. However, this information must also be present in the document in machine-readable form, so that a) its presence can be validated and b) the viewer software can exploit it.
[9] Whether there will be multiple copies of the documents in case of more than one recipient, or one single occurrence with multiple links to it is left open to the implementation. The examples shown in Chapter §5.7 stipulate the single-document-version.

transactions where all recipients are fully identifiable, and leave it to the Data Provider to provide a valid list of recipients. [10]

## §5.2 Transaction: SubmitLaboratoryReportXDS

This Transaction handles the principal lab report submissions for the Data Sharing scenario (XDS), by adding one lab report to the Registry and Repository. The report can be partial or complete. Optionally a reference to a previously submitted lab report can be added, in which case the new report replaces the previous one. As replaced reports become deprecated this means that only the last report submitted in a series is valid and visible for Data Consumers.

### Input

| | | |
|---|---|---|
| Transaction ID | 1 | UUID |
| Patient Identification Info | 1 | see glossary entry |
| Provider Identification | 1 | see glossary entry |
| Title | 0 or 1 | text |
| Comments | 0 or 1 | text |
| Lab Report | 1 | Structured or unstructured report |
| Patient Read Blocking | 0 or 1 | Yes/No (default: No) |
| Unblocking Code | 0 or 1 | see glossary entry |
| Predecessor Reference | 0 or 1 | UUID for a lab report |
| Abnormal Results | 1 | Yes/No |

### Validation

1. Patient **Identification Info** has to be provided, even if the patient is not fully identifiable which may happen e.g. in emergency cases. Such information is always available, as the lab's LIS, and possibly the hospitals HIS systems also need some kind of patient ID, be it a temporary one.
2. **Provider Identification:** See point 2 in Validation of SubmitLaboratoryReportXDR.
3. **Title, Comments:** See point 3 in Validation of SubmitLaboratoryReportXDR.
4. **Lab Report:** See point 4 in Validation of SubmitLaboratoryReportXDR.
5. The **Patient Read Blocking** flag and **Unblocking Code:** See "Patient Read Blocking Flag and Unblocking Code" at the beginning of Chapter **§5.**
6. The optional Predecessor Reference consists of one document UUID referring to a previously submitted document for the same patient.
7. **Abnormal Results:** See point 5 in Validation of SubmitLaboratoryReportXDR.

### Processing

1. The system uses the **Patient Identification Info** to find a unique match for a patient in the system's Patient Registry. If a unique patient match is found then the patient's consent situation is examined. If a unique patient match was not found, or if the patient has no positive consent situation, then there is no way to store and share the lab report in eSanté. Therefore the whole transaction fails with an appropriate error message.
2. A registry entry for the **Lab Report** is established, using parts of the report's header information and metadata from the present transaction. The entire report is then stored in

[10] How the Data Provider obtains and maintains a list of valid recipients is not specified in this document, and should be addressed elsewhere, because it is a common concern for all kinds of Data Providers in the whole eSanté system.

the patient's longitudinal record (see §3, Overall Framework for Data Transmission and Sharing). This comprises metadata information about the **Patient Read Blocking** flag and the **Unblocking Code**, if available, see point 5 in Validation.

3. If the **Predecessor Reference** was provided the newly submitted document is considered to be a newer and more complete version of the referred-to document, which it replaces. The referred-to document becomes deprecated and is no longer visible to normal users.
4. All users who have subscribed to the Notification Service for the arrival of new lab reports are notified by email.

### Output

See Output of SubmitLaboratoryReportXDR

### Notes

1. Transaction failure: see point 1 in the Notes of SubmitLaboratoryReportXDR.
2. All lab reports that belong to a series (i.e. contain results ordered in the same prescription) should normally be issued as 0, 1 or more partial results followed by one complete report. However we will not enforce this rule when submitting the next report in a series, in order to have more flexibility on the Data Provider side. Practically this means that a complete report could be followed by a partial one, without being rejected.
3. Optionally a parent document link of the replacement type (RPLC) should be present in the **Lab Report**'s own metadata, linking it to its immediate preceding partial report. This information has to be included in the report by the Data Provider, and will not be validated by the transaction.

## §5.3 Transaction: CancelDocument

This transaction handles the cancellation of any kind of document. It works for documents submitted to eSanté by XDS- and XDR-type transactions. It puts the document in a 'deprecated' status and removes it from all the Incoming Folders where it still may be present. If the document has already been downloaded from some of the Incoming Folders a cancellation message is placed in just these folders in order to inform the recipient about the cancellation. "Silent Cancellation", i.e. removal without message, is done in the other folders.

Once canceled the original document may still reside on the platform, but cannot be accessed any more by "normal" users, due to its 'deprecated' status.

### Input:

| | | |
|---|---|---|
| Transaction ID | 1 | UUID |
| Provider Identification | 1 | see glossary entry |
| Title | 0 or 1 | text |
| Comments | 0 or 1 | text |
| Cancellation Message | 1 | text |
| To-be-canceled Document Reference | 1 | Document UUID |

### Validation

1. **Provider Identification:** See point 2 in Validation of SubmitLaboratoryReportXDR.
2. **Title, Comments:** See point 3 in Validation of SubmitLaboratoryReportXDR.

3. **Cancellation Message**: A non-empty text that should contain information about the reason of the cancellation.
4. **To-be-canceled Document Reference:** This mandatory document reference consists of a document UUID referring to a previously submitted document (XDS and/or XDR).

## Processing

1. The Registry is searched for all XDR submissions that have sent the document referred to by the **To-be-canceled Document Reference** to any number of recipients. The list of their Incoming Folders is established.
2. For each of the recipient's Incoming Folders do the following:
   Check if the to-be-canceled document is still present in the Incoming Folder.
   1.1 Yes: the document hasn't yet been downloaded and viewed by the recipient. In this case simply remove it from the folder, which results in a "silent cancellation".
   1.2 No: the document has already been downloaded. A platform-generated document containing the **Cancellation Message**[11] is placed in the Incoming Folder to actively inform the recipient of the document's cancellation.
   This message contains the canceled document's title and it's unique reference (UUID).
   Example:
   > The Complete Lab report entitled "Bacteriology" from "Lab Tests Online" and identified by the unique ID u***rn:uuid:bcf45a09-9d34aef5-98ea-c5fae28db201*** has been canceled.
   > Reason: Report associated with wrong patient.

   Notice that this procedure works also if the to-be-canceled document has already been entirely removed from the platform, e.g. after its deletion due to the absence of patient consent.
3. If the to-be-canceled document still exists on the platform, it is given the status 'deprecated', independent from its current status. This makes it unavailable for viewing by normal XDS Data Consumers such as the prescriber and the patient.
4. All concerned users (patient, recipients) who have subscribed to the Notification Service for document cancelling & replacement are notified by email, using the **Cancellation Message** text as content.

## Output

See Output of SubmitLaboratoryReportXDR.

A positive outcome ('Success') of the transactions means that the document has been successfully canceled, and that cancelling messages and notifications have been sent as required.

## Notes

1. Transaction failure: see point 1 in the Notes of SubmitLaboratoryReportXDR.
2. This transaction is general enough to be used for any kind of document canceling, and not just limited to laboratory reports.

[11] See the point 5 in the Notes.

3. This transaction is focused on the cancellation of one given document in its current submission context (patient for XDS, recipients for XDR) and does therefore not need to be given any patient or recipient identification information, as is necessary for XDS and XDR transactions.
4. It is possible to cancel an already deprecated document, without transaction failure. In such a case the already canceled document is simply left in its deprecated state, and new cancelling messages and notifications are triggered.
5. **Notifications and Messages:** we distinguish between notifications and messages. Although the intent is similar, they are delivered by two completely different and independent mechanisms of the platform:
   - N**otifications** are events that the user has to subscribe to in order to receive them (see §6.5 Notification Subscription Change). He also needs to provide a valid email address to get them delivered (push mechanism). Notifications can be received by all users, i.e. patients and HCPs.
   - **Messages** are special documents that are internally generated by platform and placed in a recipient's Incoming Folder (XDR-transmitted). They can be downloaded by the targeted recipients together with all other documents destined to them (pull mechanism). Messages can only be received by HCPs through their Incoming Folder.

   The sending of messages is not a precondition for sending notifications. All users who have subscribed to the appropriate notification event will receive such a notification, even in case of a silent cancellation.
6. Document cancelling may result in the deletion of the document, if the patient has no consent. However, the physical deletion of the document itself is not a direct consequence of the CancelDocument transaction, even though the removal of the document from all Incoming Folders may have created the condition required for physical document removal. The deletion itself is the consequence of the lack of patient consent, and is dealt with by a different service of the eSanté platform (see [LABO WP5 CDC Technique], which introduces the notion of a "Lifecycle-Service " to remove expired documents).

## §5.4 Transaction: ReplaceDocumentXDR

Sends one replacement document for a previously XDR-submitted document to a list of identified recipients. The document to replace is removed from all Incoming Folders where it still may be present. If it has already been downloaded from some of the Incoming Folders a replacement message is placed in just these folders in order to inform the recipient about the replacement. "Silent Replacement", i.e. removal without message, is done in the other folders.

The document to replace may or may not have been deprecated before (i.e. canceled or replaced).

### Input:

| | | |
|---|---|---|
| Transaction ID | 1 | UUID |
| Recipient Identification Info | 1 or more | see glossary entry |
| Provider Identification | 1 | see glossary entry |
| Title | 0 or 1 | text |
| Comments | 0 or 1 | text |
| Replacement Message | 1 | text |
| To-be-replaced Document Reference | 1 | Document UUID |
| Replacement Document | 1 | Document |
| Abnormal Results | 1 | Yes/No |

## Validation

1. to 3. For **Recipient Identification, Provider Identification, Title, Comments:** See Validation of SubmitLaboratoryReportXDR.
4. **Replacement Message:** See point 3 in Validation of CancelDocument.
5. The mandatory **To-be-replaced Document Reference** consists of a document UUID referring to a previously submitted document.
6. The **Replacement Document** is a new document in a format acceptable to the platform.
7. **Abnormal Results:** See point 5 in Validation of SubmitLaboratoryReportXDR.
8. **Patient Identification Data in document content:** See point 6 in Validation of SubmitLaboratoryReportXDR.

## Processing

1. Based on the **Recipient Identification Info** the list of the Incoming Folders of all recipients is established.
2. For each of the recipient's Incoming Folders do the following:
   Check if the to-be-replaced document is still present in the Incoming Folder.
   - 2.1 Yes: the document hasn't yet been downloaded and viewed by the recipient. In this case simply remove it, which results in a "silent replacement" of the document in the recipient's Incoming Folder.
   - 2.2 No: the document has already been downloaded. Therefore a platform-generated document containing the **Replacement Message** is placed in the Incoming Folder to actively inform the recipient of the document's replacement.

   Notice that this procedure works also if the to-be-canceled document has already been entirely removed from the platform, e.g. after its deletion due to the absence of patient consent.
3. The **Replacement Document** is placed in the Incoming Folders of the recipients.
4. All concerned users (patient, recipients) who have subscribed to the Notification Service for document cancelling & replacement are notified by email, using the **Cancellation Message** text as content.

## Notes

1. Transaction failure: see point 1 in the Notes of SubmitLaboratoryReportXDR.
2. This transaction is general enough to be used for any kind of document replacement, and not limited to laboratory reports.
3. The **Replacement Document** is not checked for any similarities in respect with the replaced document. It is the Data Provider's responsibility to provide a replacement document of the correct type.
4. The present transaction can be used alone, or after a CancelDocument transaction. In this case there will be additional replacement messages and notifications.
5. No 'RPLC' linking between the original and the replacement document is done, because in a pure XDR scenario the replaced document may not even exist anymore. 'RPLC' linking falls within the responsibility of the ReplaceDocumentXDS transaction, which should always be

issued by the Data Provider together with ReplaceDocumentXDR. However, the documents themselves may have a mechanism at CDA level that allows for versioning and linking between each other.

- the 'setId' attribute contains a UUID that is shared between all documents that belong to one evolving series of documents.
- the 'versionNumber' attribute contains successive numbers, 1, 2, 3, … for each new version of the document, starting with 1 in the first original document.

It is recommended that the data source provides and manages these attributes, but this is neither enforced nor controlled by the transaction.

6. A document that has been sent to one or more wrong recipients (XDR submission) should be canceled, not replaced, and then newly submitted, via the appropriate XDR transaction. This makes the intention of correcting a recipient error much clearer. A replacement transaction should only be used to send a new version of a document to the same recipients, not to different ones.

## §5.5 Transaction: ReplaceDocumentXDS

Replaces one existing document in the patient's SPHR by another document for the same patient. This is done by deprecating the original document, and adding the new version to the Registry/Repository. A replacement document link ('RPLC') links the new version to its deprecated predecessor. The replaced document is still present but cannot be accessed any more by "normal" users, due to its 'deprecated' status.

### Input:

| | | |
|---|---|---|
| Transaction ID | 1 | UUID |
| Patient Identification Info | 1 | see glossary entry |
| Provider Identification | 1 | see glossary entry |
| Title | 0 or 1 | text |
| Comments | 0 or 1 | text |
| Replacement Message | 1 | text |
| To-be-replaced Document Reference | 1 | Document UUID |
| Replacement Document | 1 | Document |
| Patient Read Blocking | 0 or 1 | Yes/No (default: No) |
| Unblocking Code | 0 or 1 | see glossary entry |

### Validation

1. **Patient Identification Info:** See point 1 in Validation of SubmitLaboratoryReportXDS.
2. **Provider Identification:** See point 2 in Validation of SubmitLaboratoryReportXDR.
3. **Title, Comments:** See point 3 in Validation of SubmitLaboratoryReportXDR.
4. **Replacement Message:** See point 3 in Validation of CancelDocument.
5. The mandatory **To-be-replaced Document Reference** consists of one document UUID referring to a previously submitted document for the same patient.
6. The **Replacement Document** is a new document for the same patient.
7. **Patient Read Blocking** and **Unblocking Code**: See point 5 in Validation of SubmitLaboratoryReportXDS.
8. **Abnormal Results:** See point 5 in Validation of SubmitLaboratoryReportXDR.

9. **Patient Identification Data in document content:** See point 6 in Validation of SubmitLaboratoryReportXDR.

## Processing

1. Matching **Patient Identification Info** with Patient Registry, positive patient consent: See point 1 of SubmitLaboratoryReportXDS.
2. The Registry is searched for the document referred to by **To-be-replaced Document Reference**. If the document does not exist the transaction fails with an appropriate error message.
3. The **Replacement Document** must be of the same type than the document referred to by **To-be-replaced Document Reference**, and belong to the patient found in processing step 1, otherwise the transaction fails.
4. Determine the status of the document referred to by the **To-be-replaced Document Reference**. If the status is
   4.1 'approved', than the status is set to 'deprecated', making it unavailable for viewing by normal Data Consumers.
   **4.2** 'deprecated', than the document has already been canceled or replaced before. This is not allowed by IHE[12], and the transaction therefore fails.
5. The **Replacement Document** is registered in the eSanté platform, with status 'approved'. This comprises metadata information about the **Patient Read Blocking** flag and the **Unblocking Code**.
6. A registry document link of the replace type ('RPLC') is established between the new document and the replaced one.
7. All concerned users (patient, recipients) who have subscribed to the Notification Service for document cancelling & replacement are notified by email, using the **Replacement Message** text as content.

## Output

See Output of SubmitLaboratoryReportXDR.

## Notes

1. Transaction failure: see point 1 in the Notes of SubmitLaboratoryReportXDR.
2. This transaction is general enough to be used for any kind of document replacement, and not limited to laboratory test reports.
3. A document that has been put in the wrong SPHR by an XDS submission due to an erroneous patient identification should first be canceled, than resubmitted via the appropriate XDS transaction, but not replaced by use of the present transaction. This makes the intention of correcting a patient error much clearer. A replacement transaction should only be used to replace a new version of a document in the same SPHR, not moving it to a different one.

[12] IHE ITI TF3 Rev7, p. 11, line 16: "Only the most recent version of a document shall be replaceable. The most recent version of a document carries a status of Approved while older versions carry a status of Deprecated."

## §5.6 Transaction: QueryDocumentReaders

In case of cancellation or replacement of an already submitted document (CancelDocument, ReplaceDocumentXDR, ReplaceDocumentXDS) labs need to know which recipients and Data Consumers have already seen the now obsolete document, in order to take their own corrective measures. The present transaction responds to this requirement by returning identification information that allows the lab to know who has actually downloaded and decoded the document.

### Input:

| | | |
|---|---|---|
| Transaction ID | 1 | UUID |
| Provider Identification | 1 | see glossary entry |
| Title | 0 or 1 | text |
| Comments | 0 or 1 | text |
| Document Reference | 1 | Document UUID |

### Validation

1. **Provider Identification:** See point 2 in Validation of SubmitLaboratoryReportXDR.
2. **Title, Comments:** See point 3 in Validation of SubmitLaboratoryReportXDR.
3. **Document Reference:** This mandatory document reference consists of a document UUID referring to a previously submitted document (XDS and/or XDR).

### Processing

1. An empty **List of Readers** is initiated. Each element of that list will contain textual information that allows the unique identification of an eSanté platform participant. Depending on the participant's role in the system this can be:
   - HCPs: name, first name, specialty, CNS code
   - Patient: the text 'PATIENT'[13]
   - For any other non-HCP participant who might have access to a patient's SPHR, such as trusted family members, legal guardian, etc. only the role or capacity in which they had access to the report can be given, such as 'GUARDIAN', 'FAMILY MEMBER' etc.[14]

**XDR Submitted Documents**

2. The Registry is searched for all XDR submissions that have sent the document referred to by the **Document Reference** to any number of recipients. The list of their Incoming Folders is established.
3. For each of the recipient's Incoming Folders do the following:
   Check if the referred-to document is still present in the Incoming Folder.
   - 3.1 Yes: the document hasn't yet been downloaded and viewed by the recipient. In this case do nothing
   - 3.2 No: the document has already been downloaded, and possibly viewed: Add the required information about the owner of the Incoming Folder to the **List of Readers**

[13] For security reasons we suggest to treat the patient as a special case, i.e. not to return detailed identification info for him, but simply state that it is the patient himself. The lab knows anyway who the patient is.
[14] Those roles are still to be worked out, which will be part of the eSanté 2 workpackage dealing with consent management.

Notice that this procedure works also if the referred-to document has already been entirely removed from the platform, e.g. after its deletion due to the absence of patient consent.

**XDS Submitted Documents**

4. The registry is searched for a document entry that corresponds to the **Document Reference**. If such an entry is found, the Registry will establish the list of all platform participants that have downloaded the document, and add for each of them an element to the **List of Readers**, according to point 1.

## Output

The **List of Readers** is returned as the result of the transaction.

## Notes

1. Transaction failure: see point 1 in the Notes of SubmitLaboratoryReportXDR.
2. This transaction is general enough to be used as a request to establish the readership of a document, not just for lab reports.
3. This transaction is focused on the retrieval of information of one given document in its current submission context (patient for XDS, recipients for XDR) and does therefore not need to be given any patient or recipient identification information, as is necessary for XDS and XDR submission transactions.

## §5.7 Examples and illustrations

This Chapter develops three scenarios that illustrate the usage of the main Labo transaction : *SubmitLaboratoryReportXDS*, *ReplaceDocumentXDS*, *SubmitLaboratoryReportXDR*, *ReplaceDocumentXDR*, and *CancelDocument*.

1. Submission of a partial report followed by a complete report with XDS transactions, then replacement of the complete report by a corrected version;
2. Same as the first scenario, but with the corresponding XDR transactions;
3. Building on a situation where two reports have been submitted both by XDS and XDR, the second report is cancelled, without replacement.

Each illustration represents the application of a transaction, depicting the transaction at the top of the picture, and below the state of the eSanté Registry & Repository after the successful termination of the transaction.

### Scenario 1: SubmitLaboratoryReportXDS and ReplaceDocumentXDS

Figure 5 shows the submission to the patient's SPHR of the first partial report, PR1, within a series of reports for a lab test prescription. As a result of the transaction the metadata is extracted and stored in the Document Registry, while the document is stored in the Repository. Data Provider generated UUIDs are used as transaction ID ($UUID_{Trans1}$) and as document ids ($UUID_{PR1}$). Notice the 'approved' status of the newly created Document Registry entry. Notice also that the direct line between the document and the Patient Registry actually represents an indirect link, meaning that the patient reference in the document is actually a pseudonym that can only be resolved by the TTP, which acts as the Patient Registry in eSanté.

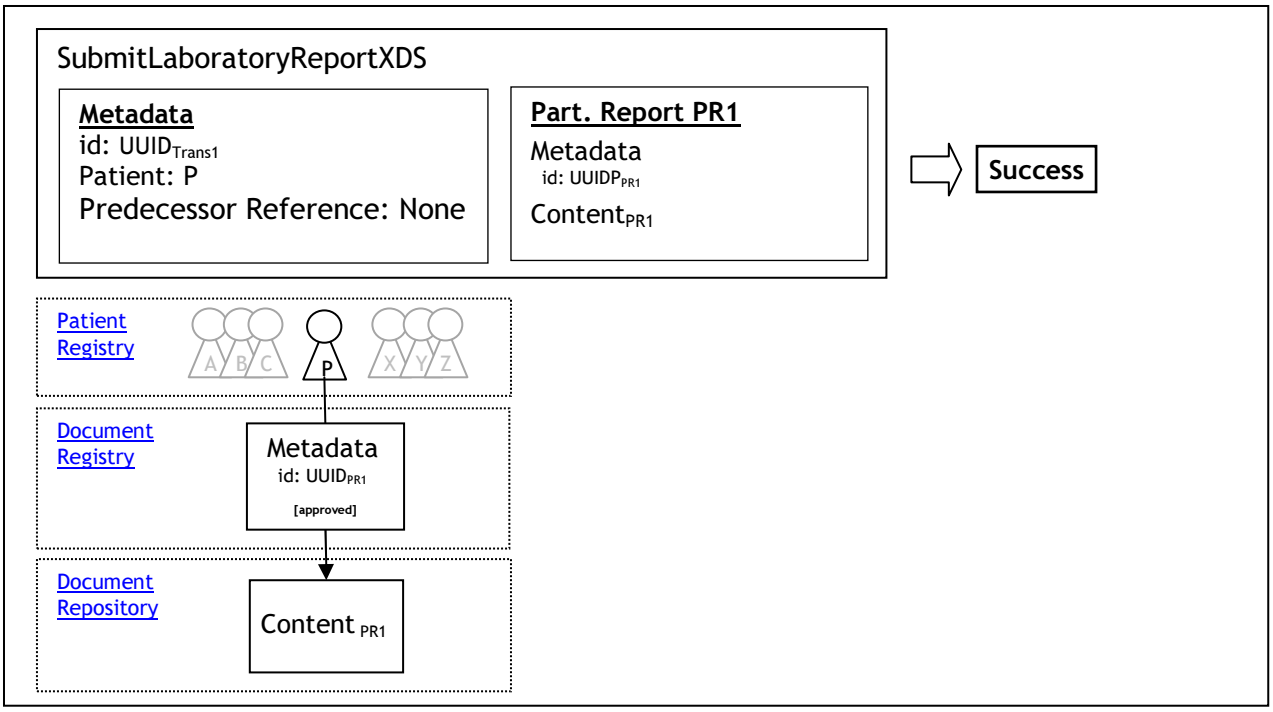



**Figure 5: Submitting first Partial Report via XDS**

Building on the previous step, a second *SubmitLaboratoryReportXDS* transaction is used in Figure 6 to submit the complete report CR1, which replaces the partial report, PR1. This is done by passing PR1's reference, $UUID_{PR1}$, as the Predecessor Reference parameter. The result is that PR1 becomes 'deprecated', i.e. invisible to Data Consumers, and in its place we find CR1, the new version. A replace link (type 'RPLC') is established between CR1 and PR1. The replaced report PR1 is still physically stored on the platform, but no longer accessible. This is graphically expressed by graying out the deprecated document's Registry entry.

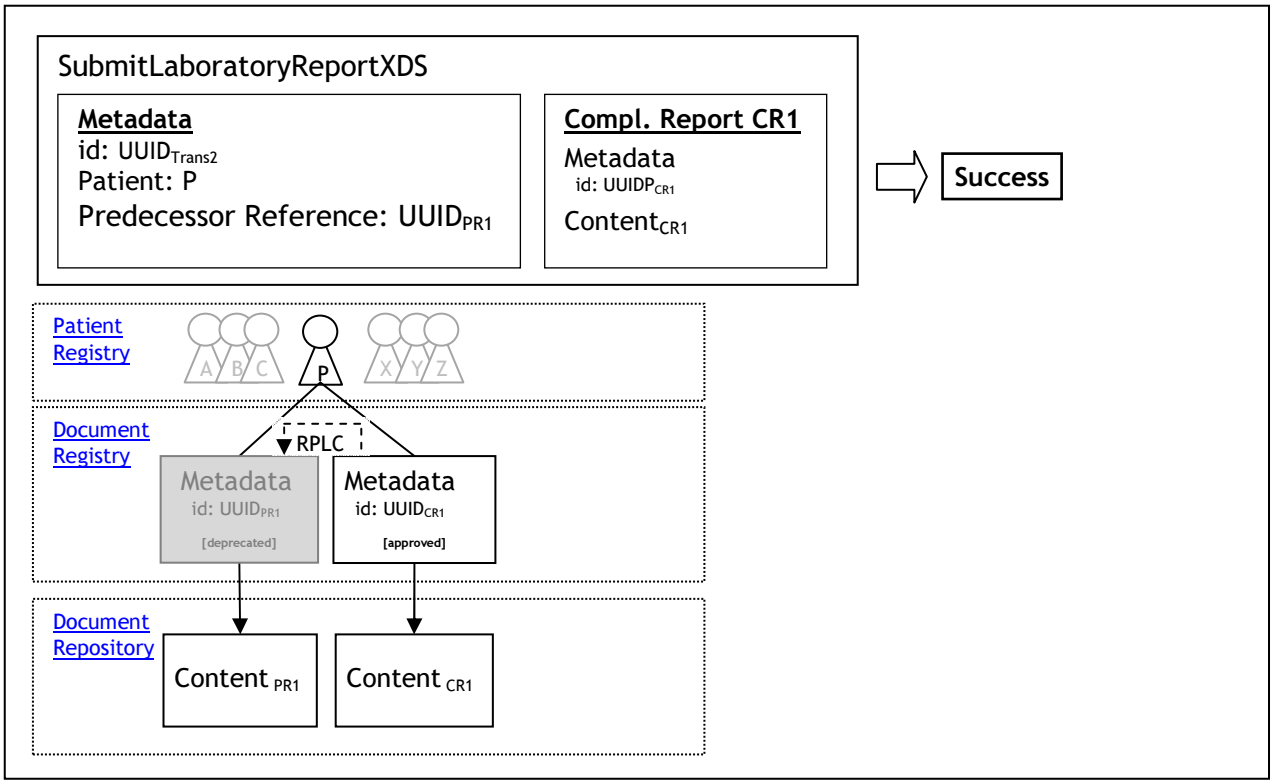



**Figure 6: XDS - Submitting Complete Report CR1 thereby replacing partial Report PR1**

Continuing this scenario in Figure 7, the complete report CR1 is now explicitly replaced using the *ReplaceDocumentXDS* transaction. The effect is very similar to *SubmitLaboratoryReportXDS* as shown in the Figure 6, i.e. deprecating CR1 and creating a 'RPLC' link between CR2 and CR1, but it also sends notification messages per email to notification subscribers of cancel & replacement events. Also, *ReplaceDocumentXDS* is a generic transaction, i.e. not specific to lab reports.

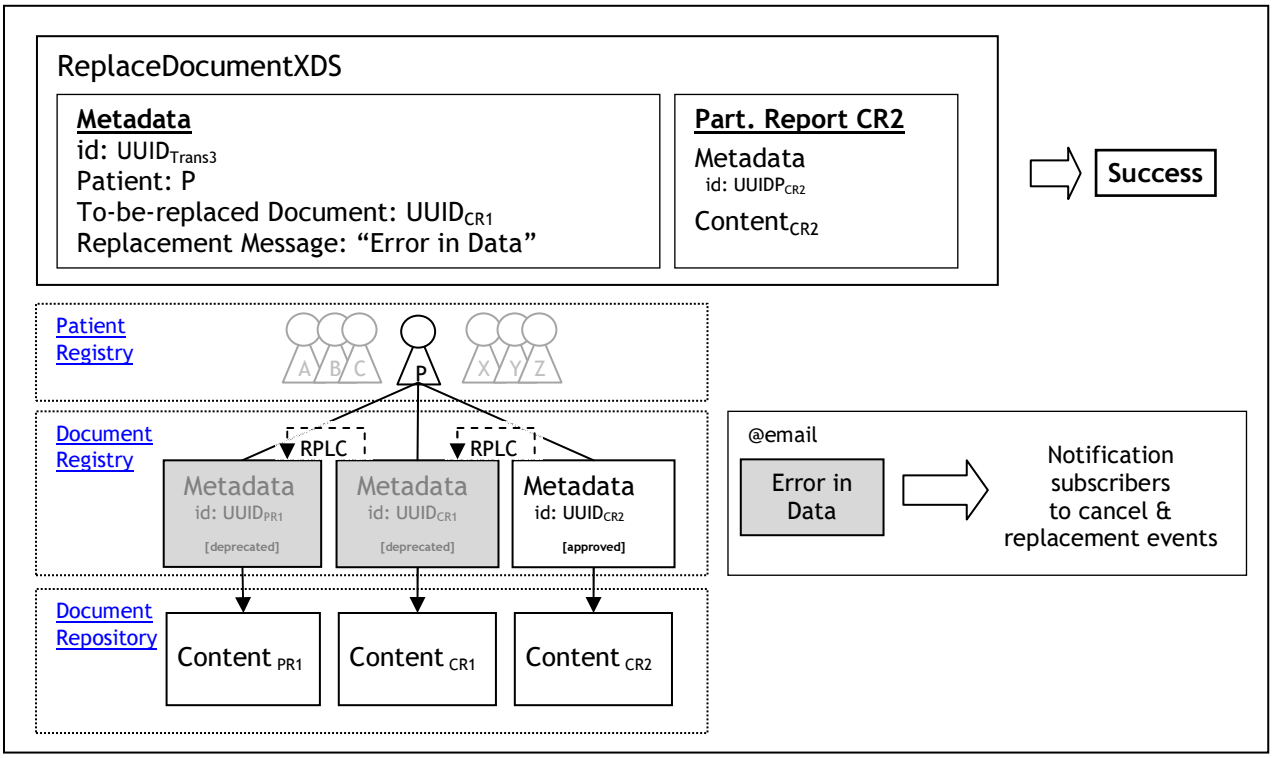



**Figure 7: XDS - Replacing an erroneous report CR1 by a corrected version, CR2**

## Scenario 2: SubmitLaboratoryReportXDR and ReplaceDocumentXDR

The next 3 illustrations replay the same submission & replacement scenario for PR1, CR1 and CR2, but in a XDR variation. The Patient Registry has systematically been left out of the illustrations, because it is not involved in XDR transactions. Instead we find the two Incoming Folders of the recipients, Dr. A and Dr. B. which will contain links to the submitted lab reports and other relevant documents.

Figure 8 submits the partial lab report PR1, and places document links to them in the Inboxes of Dr. A and Dr. B. As the example shows we have chosen to refer to only one single document in the Repository/Registry, instead of every Inbox referring to its own separate copy.

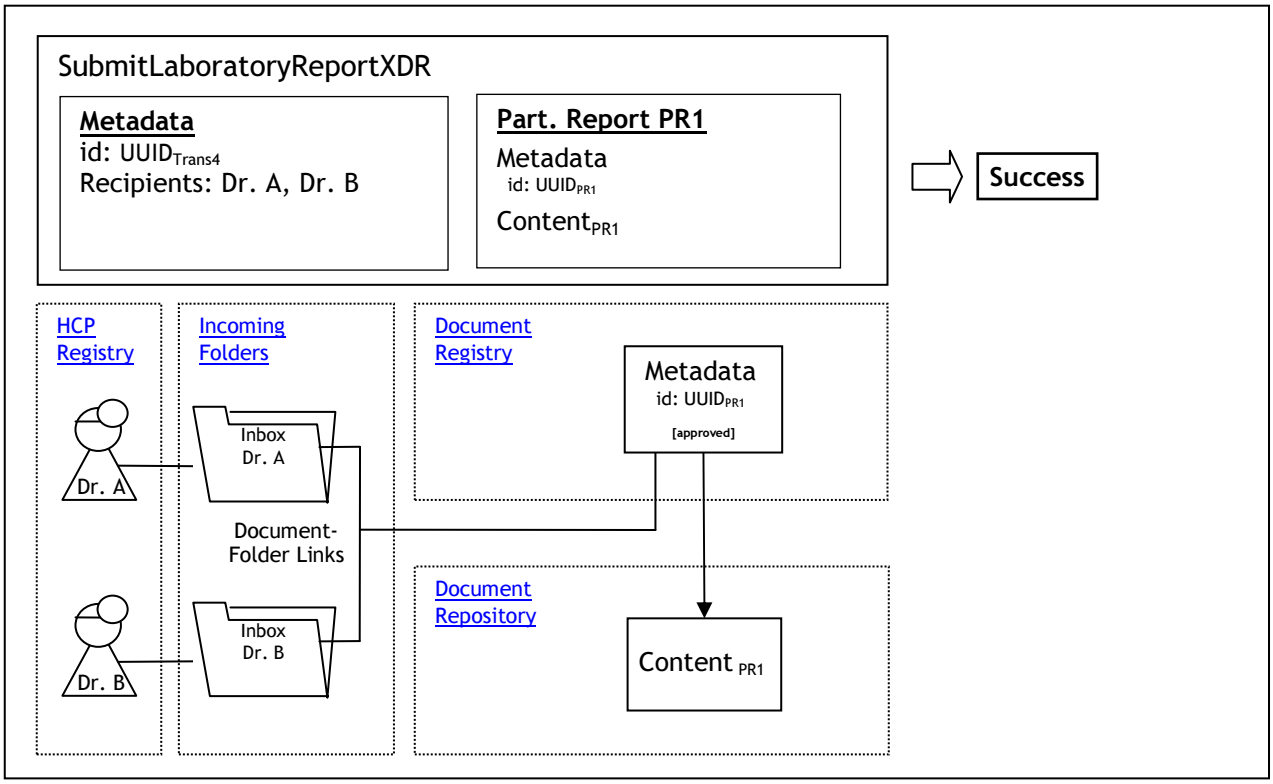



**Figure 8: XDR - Submission of Partial Report PR1**

**Note:** The multiple submission of one and the same CDA document by different transactions should be possible, too. It is e.g. assumed that a possible resubmission of PR1 will not lead to an error due to the fact that the documents have already been registered before. Instead it is verified that they indeed are identical (by hash code comparison), and if this is the case there will be no duplicate Registry/Repository entry for them.

Continuing the scenario, Figure 9 submits complete report CR1, to be sent as a new document to the recipients Dr. A and Dr. B. Other than in the equivalent XDS submission (Figure 6) there is no reference made to CR1 as a predecessor. This means that no replacement of PR1 is made, which stays exactly as it was before, including Inbox links. Therefore in XDR all submissions can be seen as independent from one another, even if the reports belong to the same prescription. PR1 and its Inbox links may or may not exist anymore on the platform, depending on whether it has been downloaded by all recipients or not. This is graphically expressed by the grey dashed lines.

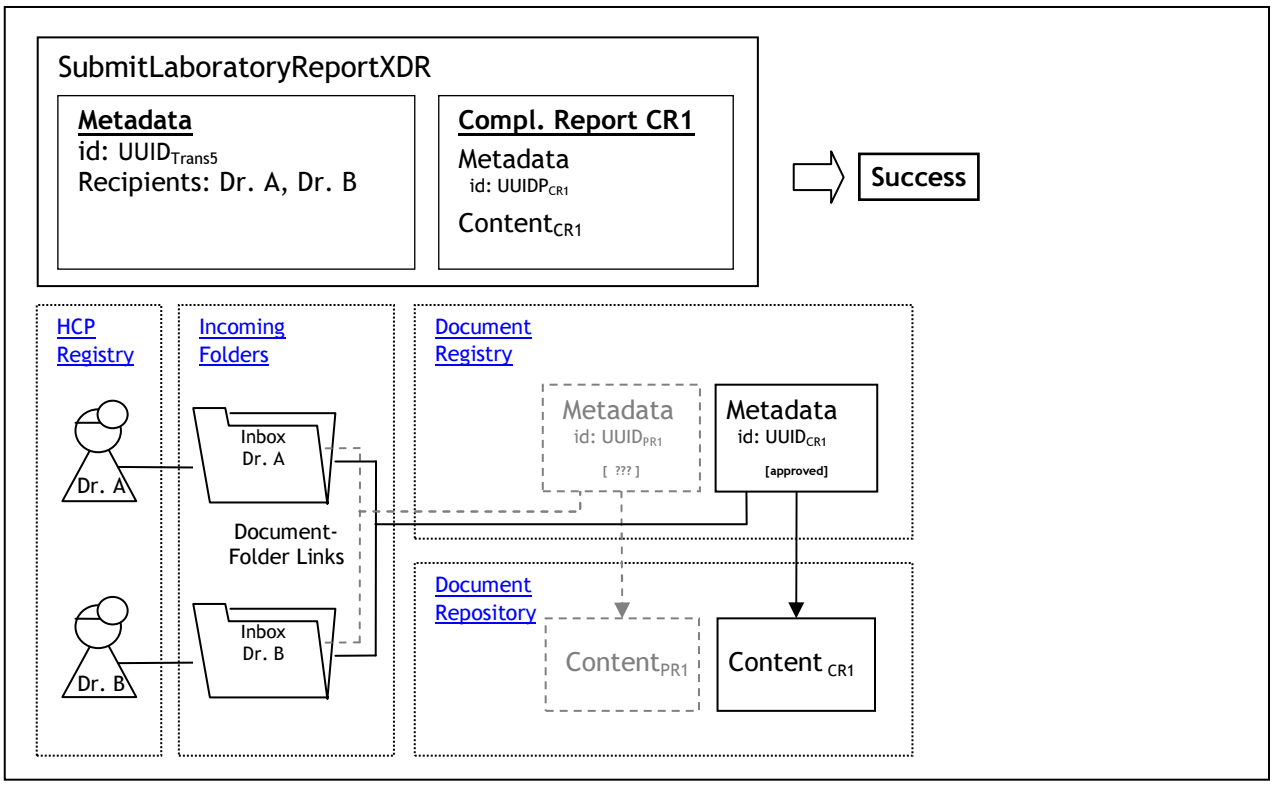



**Figure 9: XDR - Submitting Complete Report CR1**

The last step in this scenario is the XDR replacement of CR1 by CR2 (Figure 10).

While the *ReplaceDocumentXDS* transaction was in its behaviour quite similar to *SubmitLaboratoryReportXDS*, the *ReplaceDocumentXDR* transaction shown in Figure 10 differs from *SubmitLaboratoryReportXDR* in several ways.

- *ReplaceDocumentXDR* is invoked with a reference to CR1, the document to be replaced. This is necessary to find all of CR1's folder links that may still exist in the Inboxes, in order to remove them.
- If there are Inbox links to CR1, the document to be replaced, they will be removed. Two situations are possible:
  - Dr. A hasn't yet downloaded CR1, so it is "silently" replaced by CR2.
  - Dr. B has already downloaded CR1, therefore a system generated replacement message MSG1 is put in his Inbox in addition to the replacement document CR2.

Notice that only the recipients that have been specified as parameters (Dr. A, Dr. B) determine which Inboxes will receive the folder links for the replacement document and the replacement message, but not any other folder that actually contains (or contained) PR1.

As usual emails containing the text of the replacement message are is sent to eSanté users (patients, doctors) that have subscribed to the corresponding events.

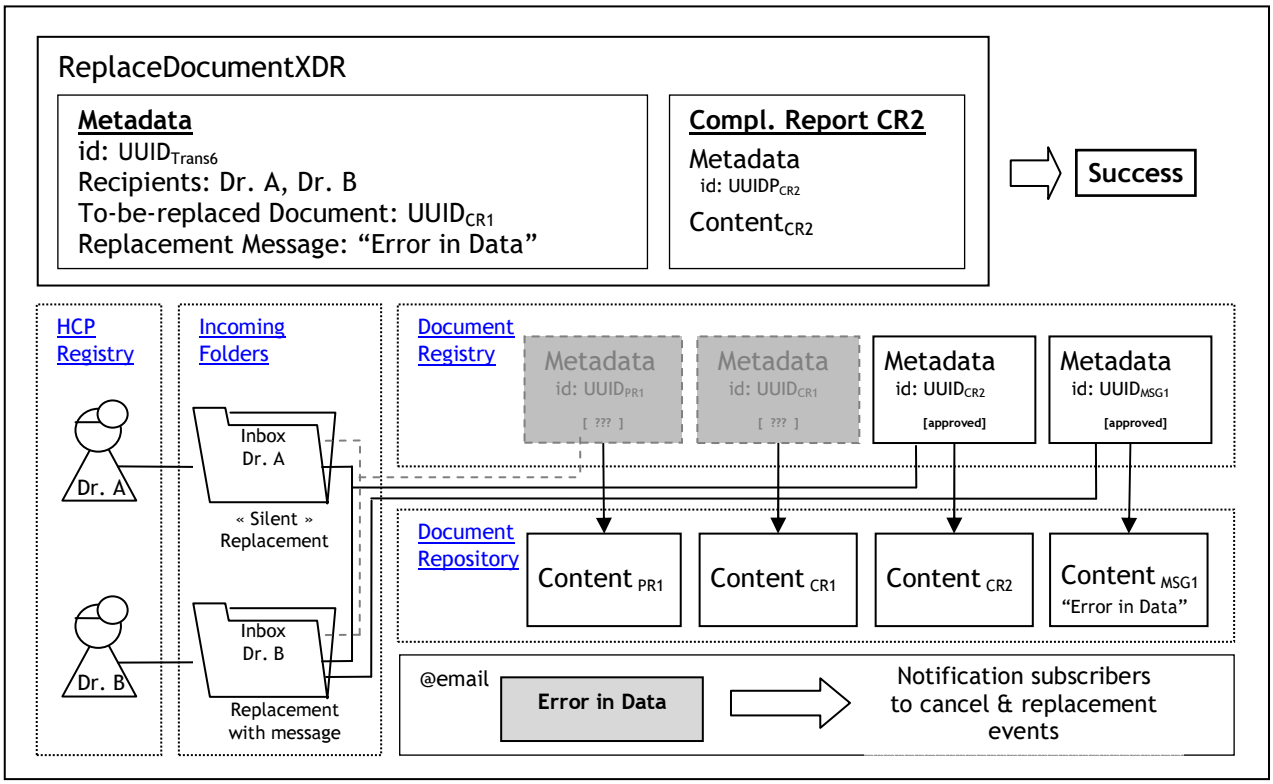



**Figure 10: Document Replacement via XDR, with and without "Silent" Replacement**

## Scenario 3: CancelDocument

Replacing a document as shown in Figure 7 (XDS) and Figure 10 (XDR) is meaningful to correct an report containing errors. There are however cases where this is not appropriate, e.g. if the report has been sent to the wrong patient, or to the wrong doctor. In such cases the only choice is cancelling the document and resubmitting it to the correct patient or doctor. The *CancelDocument* transaction is, in contrast to all other transaction illustrated so far, neither XDS nor XDR specific. This is possible because it does not submit a new document, but exclusively acts on a previously submitted one.

To show the effects of cancelling we assume a Registry/Repository state which is shown in Figure 11. Notice that CR1 has been downloaded by Dr. B, but not by Dr. A – there's still a document link towards CR1 in Dr. A's Inbox.

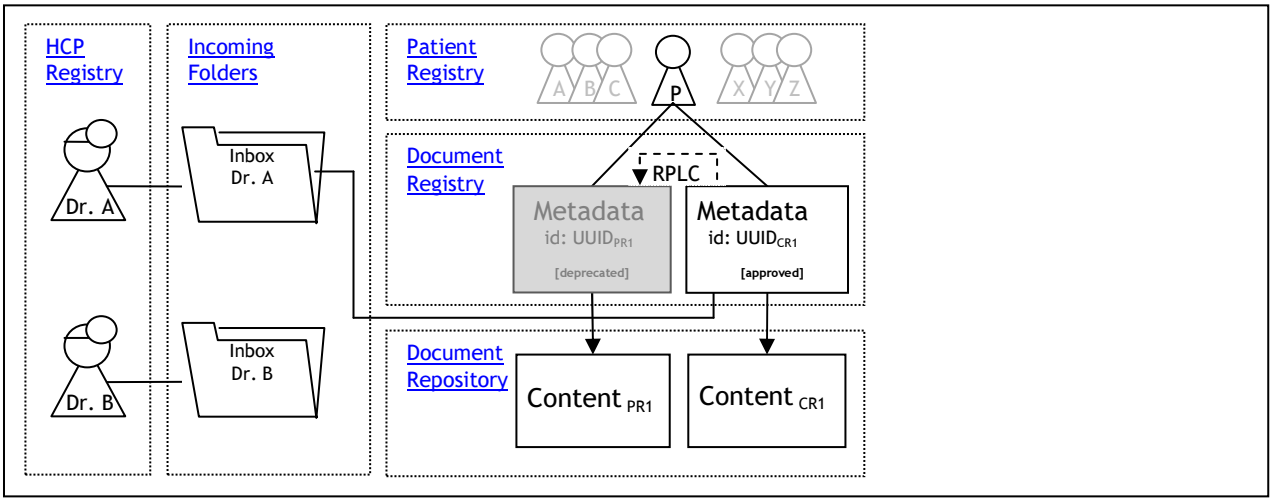



**Figure 11: State of Registry & Repository before sending the CancelDocument transaction**

Figure 12 shows the result of the transaction that cancels the complete report CR1. As we can see, the "silent" cancellation has simply removed the document link from Dr. A's Inbox. This is OK because he hasn't seen (= downloaded) the document yet. Dr. B however receives the cancellation message MSG2 in his Inbox in order to inform him, that the already downloaded document CR1 is to be ignored because of a wrong patient association.
Similar to the replace transactions an email message is also sent to all subscribers of cancelation events.

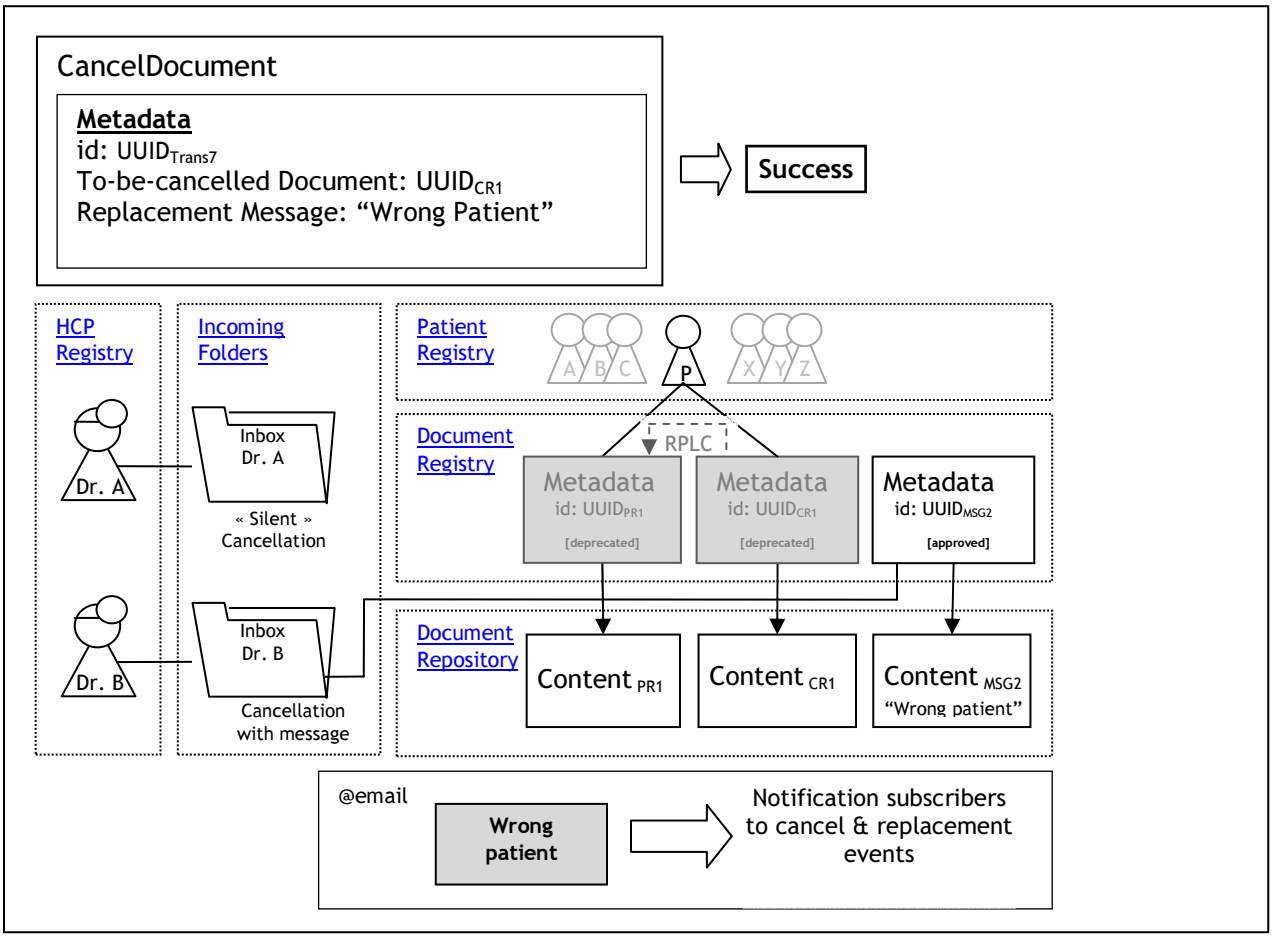



**Figure 12: Effect of the CancelDocument transaction**

# §6 Data Consumer and other functions with Mock-up-Screens

Contrary to the specification of the Data Provider side (see §5, Data Submission TransactionsData Submission Transactions), where the submission of patient data to the platform follows a rather uniform and strict schema, the Data Consumer side has more diverse functionality. A transactional description seems inappropriate at that time because it would be

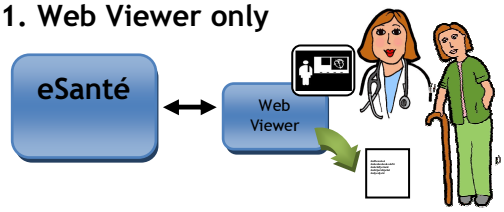
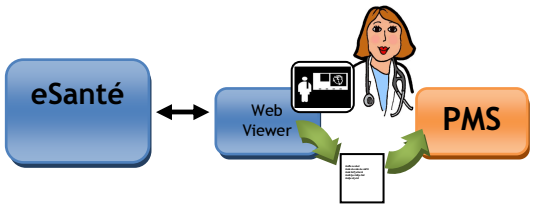
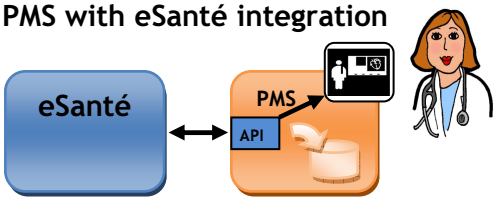
a) rather complex and difficult to understand and therefore
b) be difficult to obtain real feedback from the user community.

We have therefore opted for an approach that uses elements of a fictitious GUI, so called "mock-up screens", to describe the required functions. While the mock-up screens should help the users to get a better understanding on the system's functions, the requirements themselves are expressed in the surrounding text, enumerated in steps for easier reference. This is less formal than the specification of transactions for the Data Provider cases, but has the additional advantage to steer clear of implementation decisions, which at that stage of the analysis would be too early.

## §6.1 eSanté Web Viewer Scenarios

At this place we recall briefly the overall scenarios for eSanté Web Viewers envisioned in the LABO Use Case analysis (LABO-WP2-UseCases-v2.0, chapter §3.5 Web Viewers and Patient Management Software Integration).

Two situations have been described in which patients and HCP interact with the eSanté platform over a Web-based interface, and one with a full PMS-integrated solution for HCP only.

| | |
|---|---|
| **1. Web Viewer only**<br>  | Patients and doctors without a PMS can view and possibly download patient data from the eSanté platform through a Web viewer interface. |
| **2. PMS without eSanté integration**<br>  | Doctors with a PMS that is not integrated with the eSanté platform can view and possibly download patient data through eSanté's Web Viewer interface. If they want to keep a local copy they need to upload the files manually into their own PMS, where they attach them to the corresponding patient records. |
| **3. PMS with eSanté integration**<br>  | Doctors with eSanté integrated PMS can view and optionally download patient data directly in their own software, without manually downloading/ uploading it with the Web viewer. An Interface specification (e.g. in form of a Web API) is provided by eSanté to allow the software vendors to integrate the required eSanté functions, i.e. viewing & downloading. |

The functions described in the present chapter cover the first two scenarios, “Web Viewer Only” and “PMS without eSanté integration”. The last scenario, “PMS with eSanté integration”, is technically far more advanced and will require detailed technical specifications, and is therefore considered out of scope of this document. Also it is not easy to foresee in advance which eSanté connectivity functions the editors of existing PMS systems will chose to integrate in their own software, and how they will translate them into user level functions in their respective systems.

As a starting point the software editors should read the description of the functions presented hereafter in order to understand the functionality that eSanté will offer in its own Web Viewer interfaces, as a kind of inspiration for own developments. The idea is to provide easy access to patient data located on the eSanté platform without leaving the PMS, using demographic patient data from the PMS to automatically gain remote access to the same patient’s data on eSanté. The exact technical specifications will be made available when the actual APIs have been designed and developed.

We now turn to the description of the functionality of the eSanté Web-Viewer scenarios 1 and 2. As a means of structuring the Data Consumer functions we simply align the functional description with the corresponding use cases, namely

- LAB-UC3: §6.2 Reliable Data Transmission Viewer
- LAB-UC4: §6.3 Single Patient Data Viewer
- LAB-UC5: §6.4 Patient Data Viewer

Other functions that are used by the doctors and the patients are described in a similar way:

- LAB-UC6: §6.5 Notification Subscription Change

## §6.2 Reliable Data Transmission Viewer

For the Reliable Data Transmission the user has to perform the following steps in order to select, download, decrypt and view patient data.

1. User login and authentication vis-à-vis of the eSanté platform. A strong authentication method such as LuxTrust is mandatory, possibly in combination with a national HCP identification system.

2. Enter selection criteria for documents that have been deposited in the authenticated user’s Incoming Folder (Figure 13).

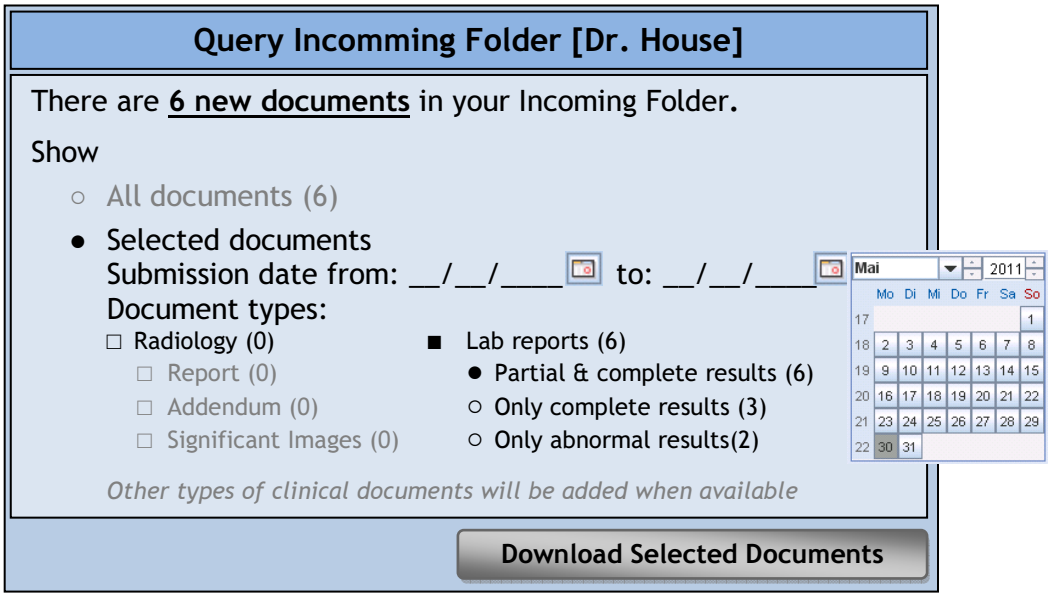



Figure 13: Doctor queries the Incoming Folder

3. The user can either choose all documents, or make more specific selections, such as a date range, different document types and subtypes[15], and specific report properties, such as abnormal results.

   The function "**Download Selected Documents**" invokes the next step 4.

4. Download and decrypt the selected documents from the Incoming Folder to the local computer (Figure 14). Notice that this operation can be interrupted at any moment. In such a case the user can re-query the Incoming Folder and restart with step 2. All the documents that have already been downloaded & decrypted have been removed from the Incoming Folder and will therefore no longer be available for download.

   There is also a maximal time limit that determines how long documents can stay in the Incoming Folder before being removed automatically. This is necessary to avoid long-term storage of patient data when it is not allowed, due to the absence of patient consent.

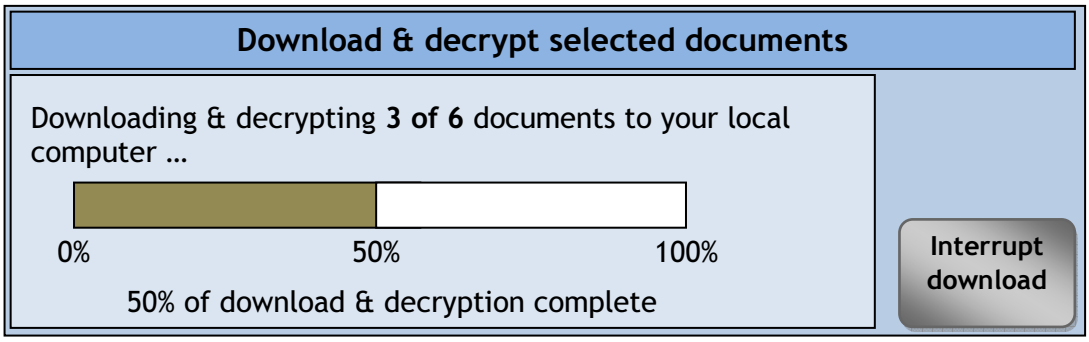



Figure 14: Download progress bar for the Incoming Folder

5. Display and browse the list of documents that have been downloaded onto the local computer, and visualize them (Figure 15). Now that the documents are locally available in

[15] In the mock-up screens of this chapter we only show radiology and laboratory relevant document types, as well as referral folders and their contents. But with further extensions of the eSanté platform more document types will become available.

decrypted form on the recipient's computer[16], and more metadata is available per document, in particular the name and matricule of the patient, the creation date and other document details (laboratory, specialty, …).

6. The **View** function ( ) allows the visualization of the document with appropriate viewer software. This is either standard software available free of charge from the Internet such as a PDF viewer, or made available through automatic download from the eSanté platform.[17] Furthermore it can be used to visualize documents that have been downloaded at an earlier moment. A presentation in chronological order with grouping by common periods (days, weeks, months, years for dates, A, B, C, D … for text) seems to be appropriate in order to manage larger numbers of downloaded documents. Ordering the list by different criteria (download date, create date, patient name, document type, origin) should also be possible.

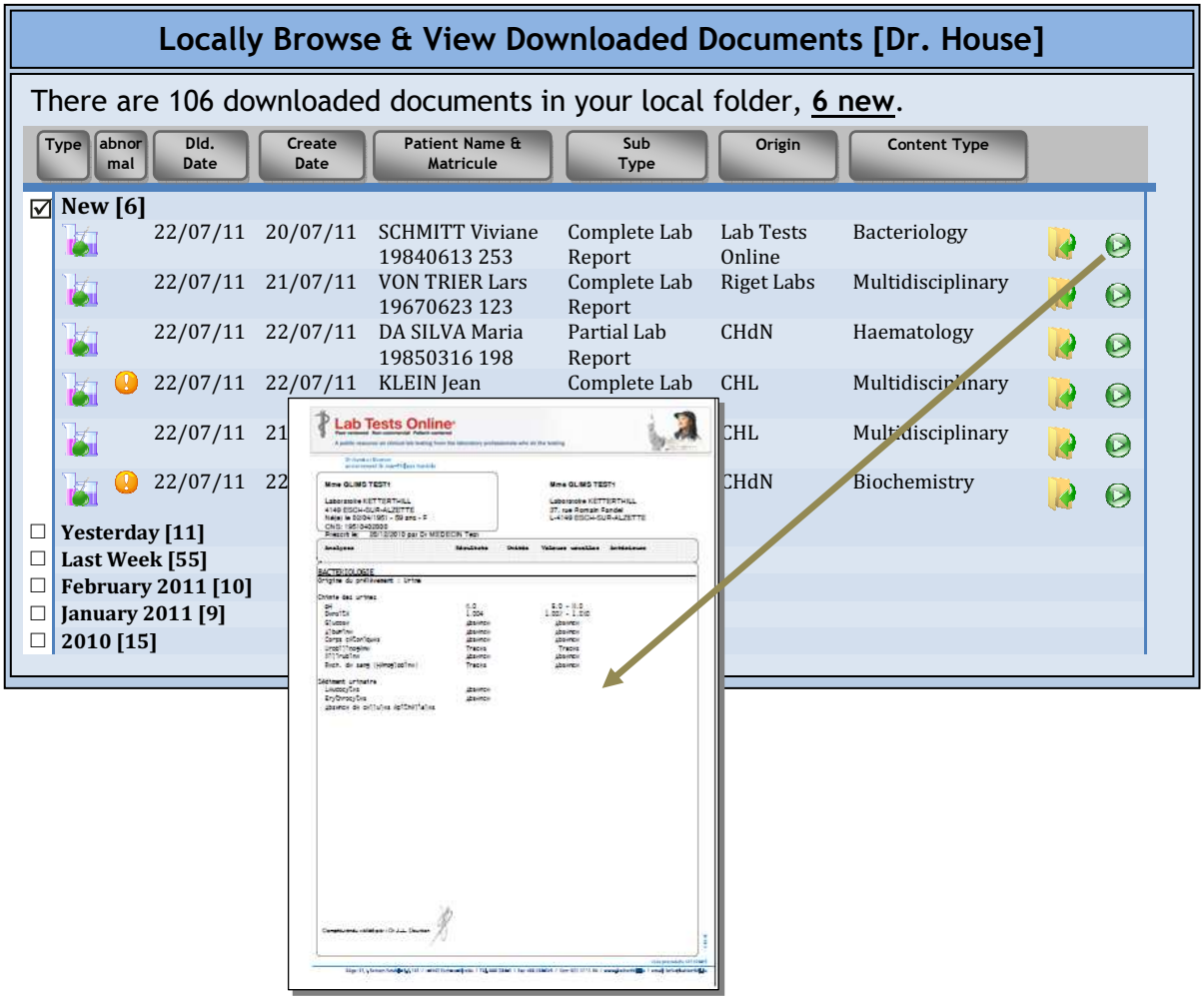



Figure 15: Doctor's browser for downloaded documents

7. The browser & viewer described in steps 5 and 6 are simple tools that help to locate and visualize medical data that has been downloaded into a temporary data storage on the user's

[16] A browser applet is capable of accessing local files on the user's computer if it has been digitally signed by the applet provider.
[17] The browser itself could be a Java applet that can be downloaded and run from within the user's Java-enabled Web browser. The viewing of individual documents depends on their format: Acrobat Reader for PDF files, HTML browser for CDA documents using style sheets for rendering.

local computer[18]. However, it is not meant to be a full-fledged organization system for medical patient files. Eventually all downloaded documents should be moved into the doctor's own PMS, or at least removed from the local download repository and stored elsewhere. The doctor's PMS should be able to attach theses documents to the patient's record, and also to use the viewer software provided by eSanté to visualize the document content.

The **Move** function ( , Figure 16) helps to do just this, by moving the file from the local download storage, where it has been placed in step 4, to an archive destination of the user's choice, where it could be picked up by the doctor's PMS. The function also suggests a renaming of the file, using document metadata as part of the new filename, to facilitate its localization by the user.

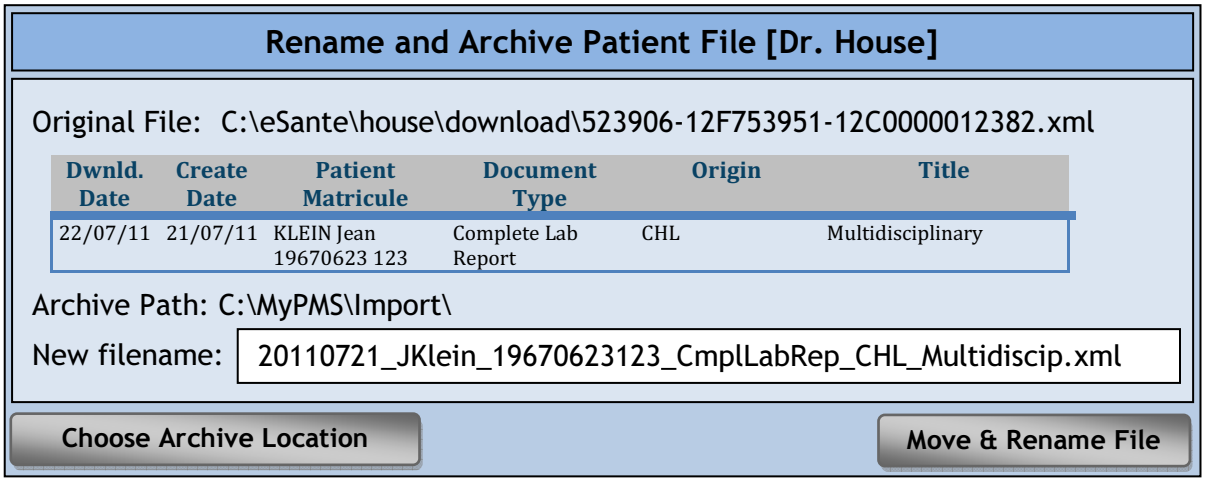



**Figure 16: Renaming and archiving of downloaded medical files**

## §6.3 Single Patient Data Viewer

To access data in a patient's SPHR the HCP has to perform the following steps to select, download and decrypt documents that are available in the patient's SPHR.

1. User login and authentication vis-à-vis of the eSanté platform. A strong authentication such as LuxTrust, possibly using a special SmartCard for HCP, is mandatory.
2. Enter patient identification information for the patient who's SPHR should be accessed. In normal circumstances it is sufficient to provide a simple patient ID, either the matricule or another officially recognized ID (Figure 17).

[18] The browser applet can be locally configured so that it knows where to store the downloaded files.

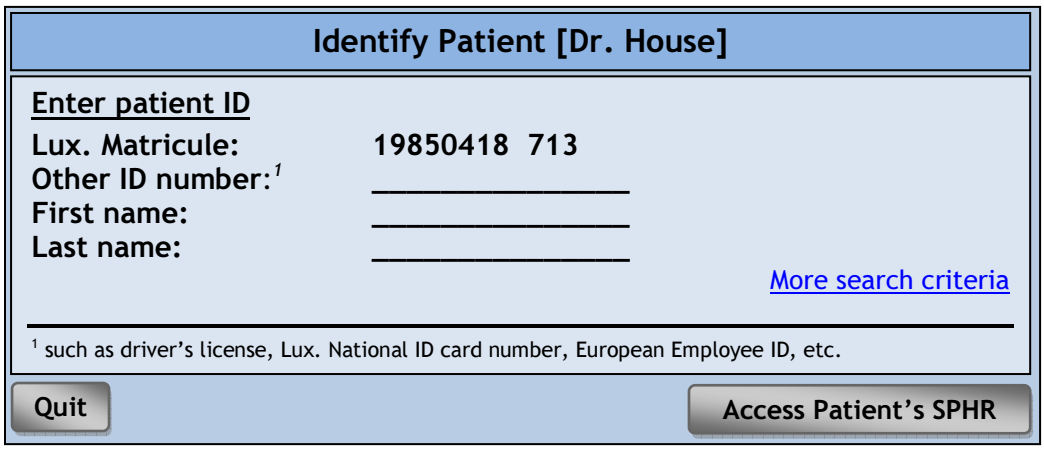



Figure 17: Simple patient identification

3. However, if those IDs are unavailable or do not exist, such as foreigners not registered with CNS or with a social security organization not known in Luxemburg, an extended set of search criteria can be used to identify the patient (Figure 18).
   In both cases the criteria entered for the patient search should result in an exact match for one and only one patient. A warning is raised if the search results in more than one patient match, or none at all, and the user is asked to provide different identification information before retrying.

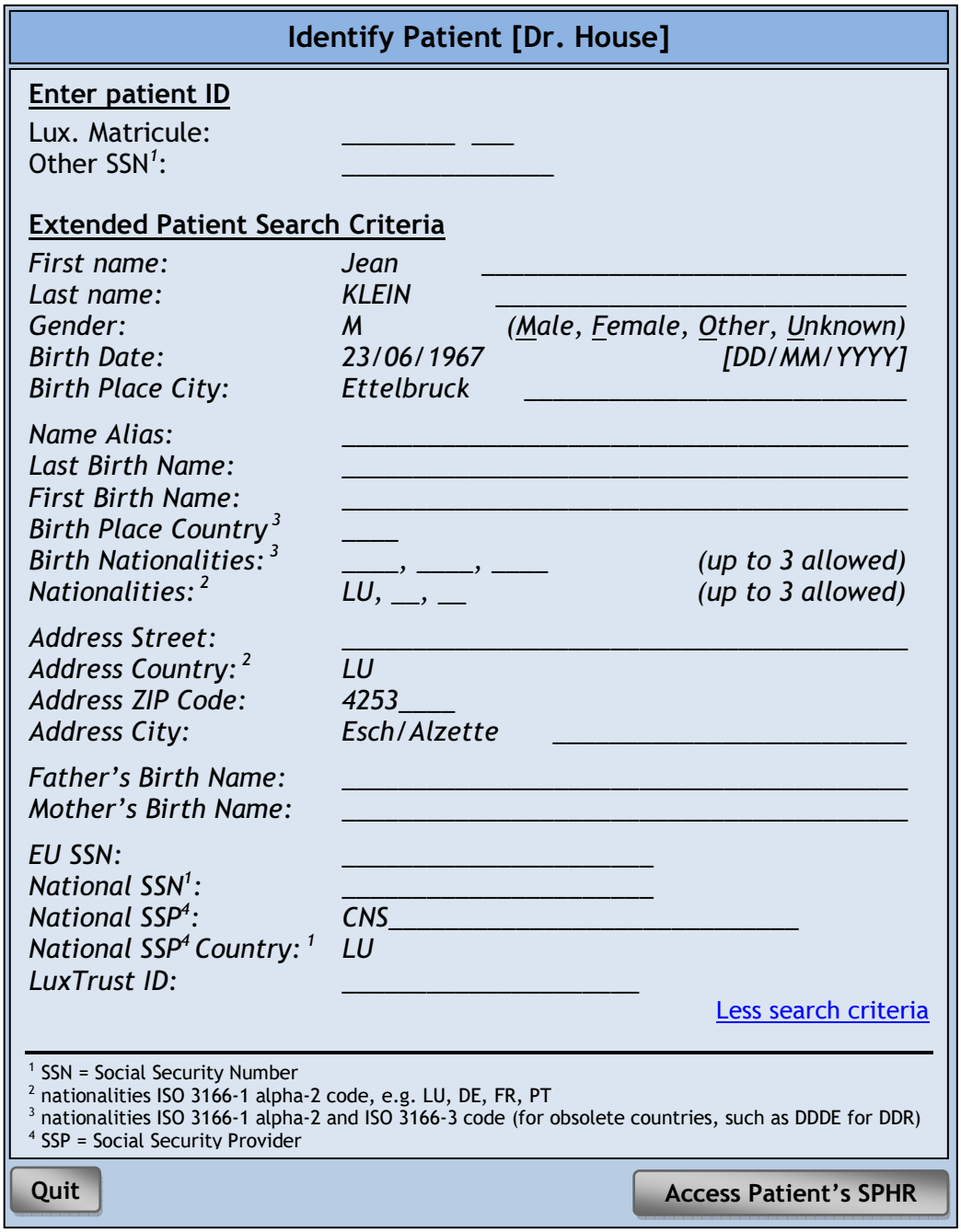



Figure 18: Extended patient search criteria

## Emergency Access

A special case must be made for emergency access to patient data on eSanté. In such situations very little may be known of a patient: name, first name, gender, birth date, birth place - basically the reliable information that is printed on a national ID card or a driver's license. In absence of more information a reliable and unique identification becomes less likely. Name misspellings and typing errors could also lead to a false patient identification.

A different *modus operandi* for patient identification should therefore be envisaged in such cases: the doctor types in the little information he has. The system then runs a "fuzzy search" against a "Citizen Registry", outside of the eSanté platform, providing a list of likely matches

with more demographic information. The doctor selects one patient among the list, thereby receiving more data identifying him uniquely ("single best record").

Emergency access to a patient's SPHR on eSanté has not yet been analyzed in detail, and is therefore out-of-scope for the present specification.

4. **Presentation of an overview of the medical data available for the patient** (Figure 19). The available data is grouped in clinical categories such as Radiology, Laboratory, etc., and special categories such as Appointments, Referral Folders, etc. If a category contains more items than can be shown, a scrollbar or paging function gives access to the older items.

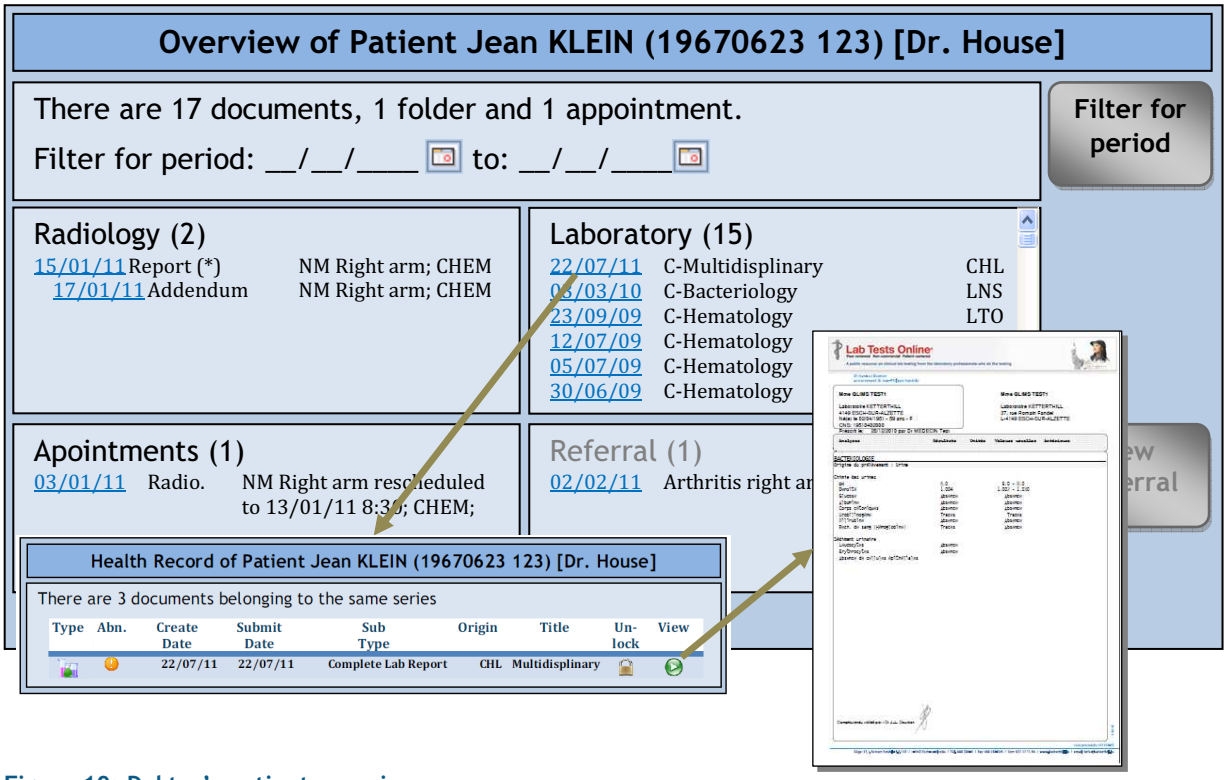



Figure 19: Doktor's patient overview

**Access to more functions on a document.**

A detailed view of the document with more metadata and additional functions to call is available for each lab report in the list view (Figure 20). This is done by clicking on a hotlink in the above screen. E.g., when clicking on the first link in the laboratory group, "22/07/11 C-Multidisplinary CHL", the following, more detailed list opens, which shows a more detailed metadata view of the report. From there the document can be opened ('View' function - ), and further functions executed (such as 'Unlock' - ).

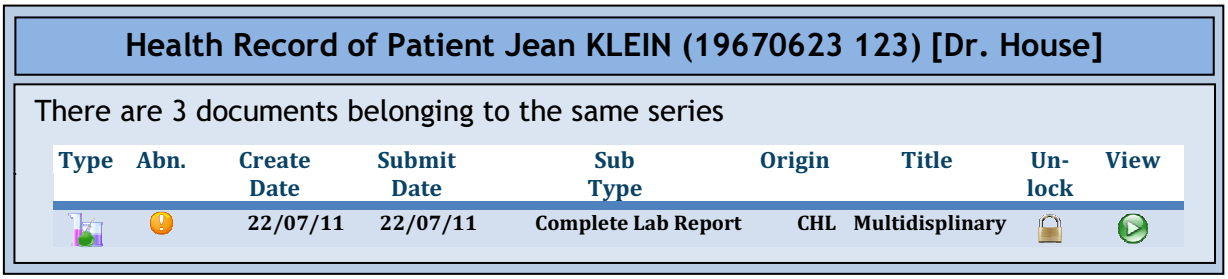



Figure 20: Metadata list view of a document

Visual decorations such as bold fonts for the principal documents, text underline for emphasis, icons for types, status etc. should be used whenever this seems appropriate.

5. The 'View' function ( ) allows to retrieve, decrypt, view and possibly download an individual document with appropriate viewer software (see step 6 of the Reliable Data Transmission Viewer).
6. The padlock symbol ( ), representing the 'Unblock' function, is present only for documents that have specifically been marked as blocked by the Data Provider. Any doctor who has access to these documents is able to unlock them and make them viewable for the patient (Figure 21).

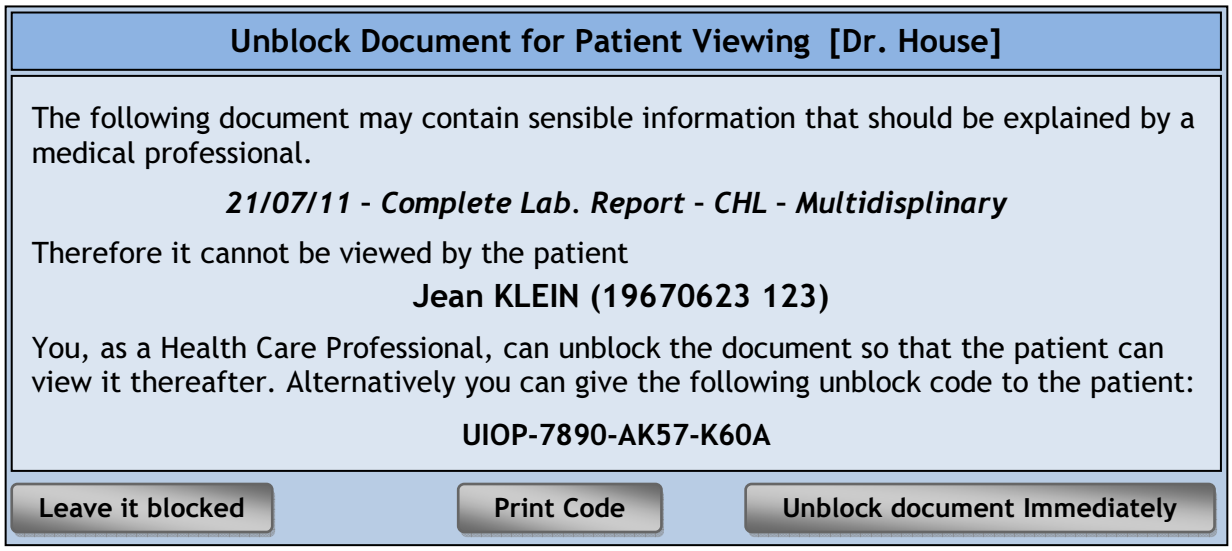



Figure 21: Doctor unblocks report for patient

No entering of the unblock code is necessary. Alternatively the doctor can print out and give the unblock code to the patient, so that he can unblock the document himself (step 3 of Patient Data Viewer).

## §6.4 Patient Data Viewer

The patient can access his own SPHR using a simplified version of the Single Patient Data Viewer. The main difference is that the patient is already identified through his login, and therefore the patient identification from step 2 is not needed. To access his own SPHR the patient has to perform the following steps.

1. Patient login and authentication vis-à-vis of the eSanté platform. A strong authentication method such as LuxTrust is highly recommended.
2. Presentation of an overview of the medical data available to the patient (Figure 22). This is nearly identical to the doctor's function in step 4 of the Single Patient Data Viewer. It may vary slightly in the categories of documents that are available, as well as in individual documents.

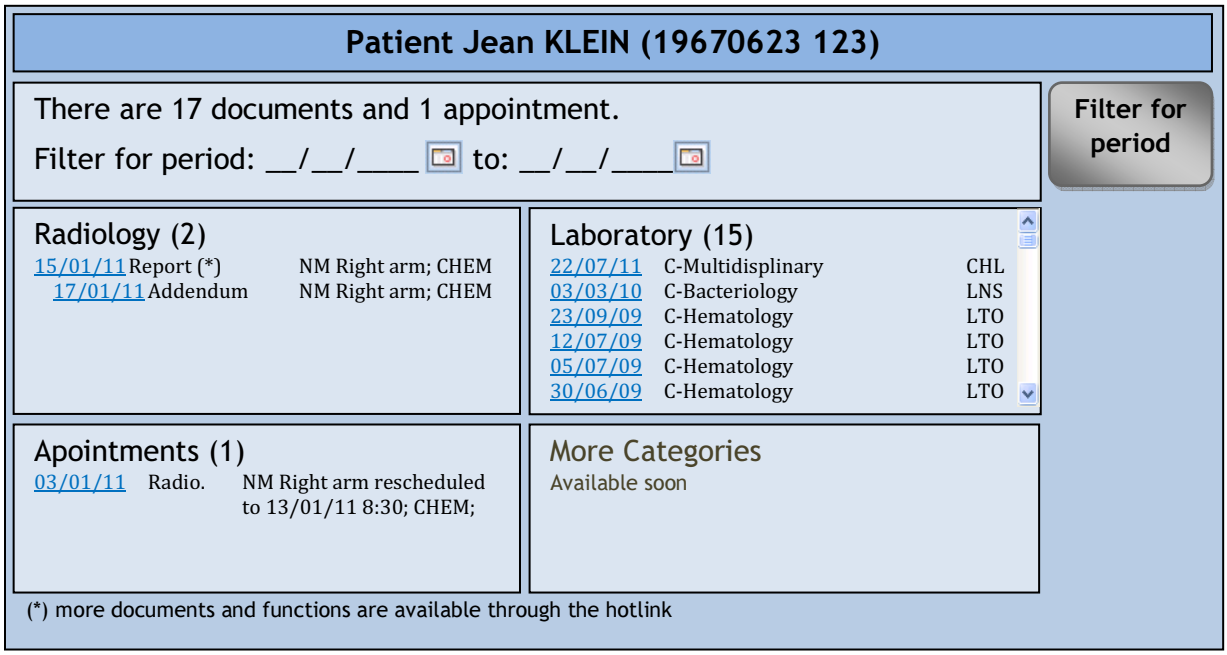



**Figure 22: Patient's overview to his own SPHR**

The document viewing function is identical or similar to step 6 of the Reliable Data Transmission Viewer, i.e. the patient can view individual documents with the downloadable viewer software provided by the eSanté system. In this example clicking on the line '22/07/11 C-Multidisplinary CHL' would open a screen like shown in Figure 20.

3. Unblock documents. Patients normally have access to their complete medical record, but some documents can exceptionally be blocked by a special demand of the prescriber. These blocked documents, must first be unlocked by a HCP before a patient can view them (see point 6 of the Single Patient Data Viewer). The patient can still see the presence of the report and some of the report's metadata, but he cannot visualize or download the report itself. By activating the 'Unblock' function (Figure 23) the patient himself can unblock the file if he has been given the correct unblock code by a HCP (see point 6 of the Single Patient Data Viewer).

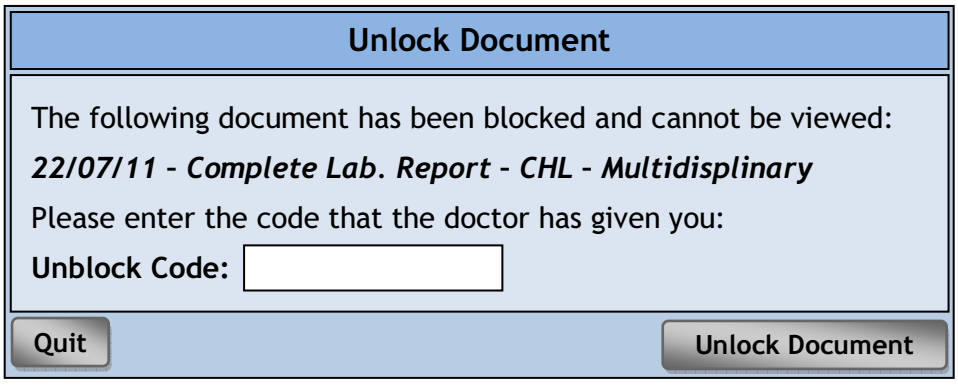



**Figure 23: Patient unblocks document**

If the patient provides an incorrect or no code at all an error is signaled to that effect, and he can have another trial or quit.

## §6.5 Notification Subscription Change

The notification subscription and unsubscription is a relatively simple process which allows a user to subscribe to and unsubscribe from predefined notification services, which are all related to events that occur on the eSanté platform.
In addition to the selection of subscribed events a user has to provide a valid email address for notification delivery, and also to confirm any changes in his notification subscription by activating a Web link, which is sent to him by email.

1. User login and authentication vis-à-vis of the eSanté platform. Same as step 1 in Single Patient Data Viewer for HCPs, respectively step 1 in Single Patient Data Viewer for patients.
2. The user is shown his current state of notification subscriptions (Figure 24). He can select (or deselect) any number of events for which he wants (or not) to be notified if they occur in the future. He also should provide a valid email address to which the confirmation and notification messages will be sent. For a doctor it is suggested that he can subscribe to events that occur in his Incoming Folder as well as in the SPHR of any of his patients, meaning any patient he is the reference doctor of.

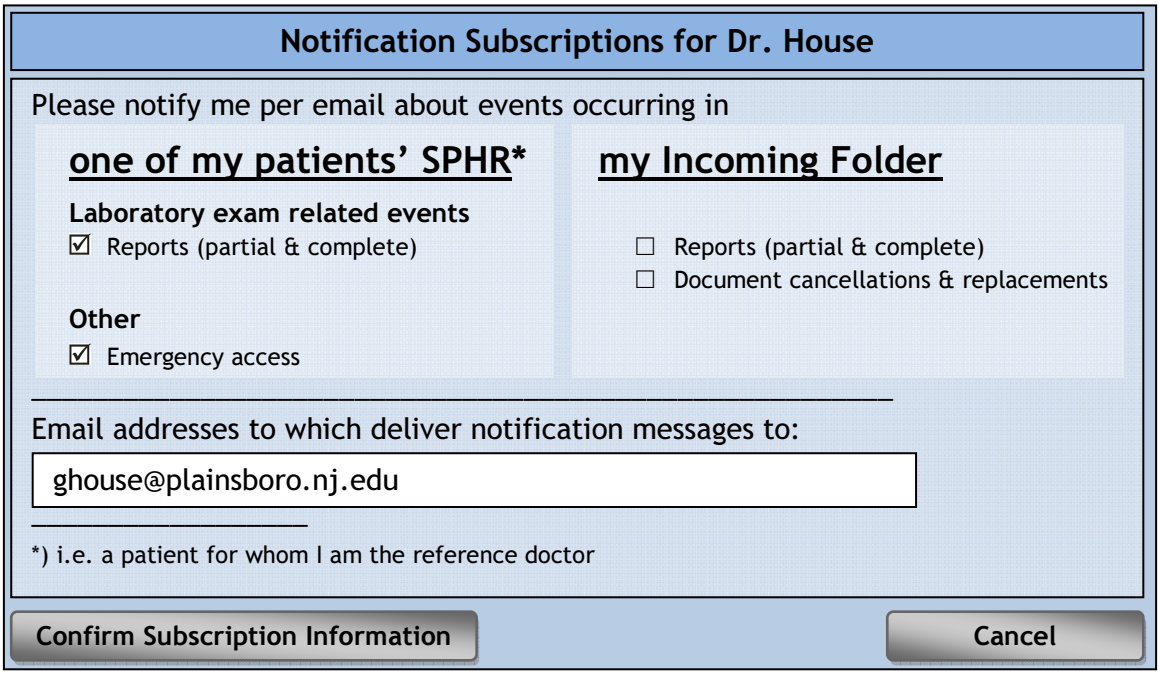



Figure 24: Notification subscription for a doctor

The patient's choice of events is simpler because he can only access his own SPHR, while a HCP can not only access all his patient's SPHRs, but also his Incoming Folder, which represents a parallel delivery channel for documents (Figure 25).

**Patient:**

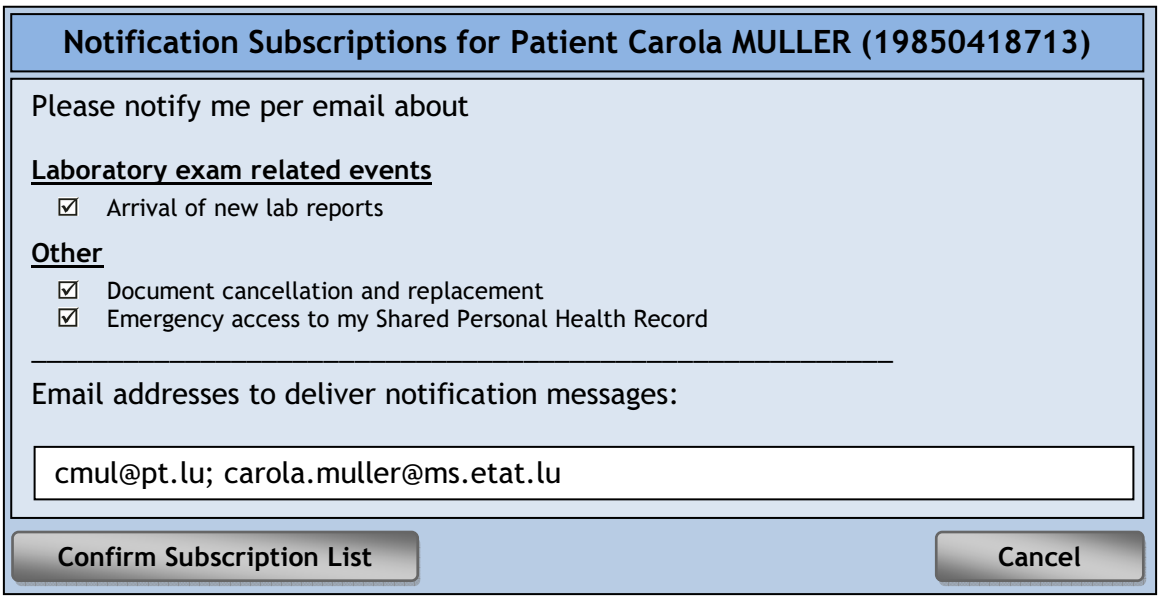



Figure 25: Notification subscription for a patient

3. When changing the state of subscription the system sends an email to the delivery address, asking the user to confirm the current state of subscriptions by activating a specific URL (Figure 26). Only if this URL is invoked the changes are taken into account.

To : cmul@pt.lu
Cc : carola.muller@ms.etat.lu
From: notification_service@esante.etat.lu
Subject: Your notification change request from 15/4/2011 13:48

You have made changes in your eSanté notification service. You have asked eSanté to be informed by email if one of the following events happens in your Shared Personal Health Record (SPHR):

- Arrival of new lab reports
- Document cancellation and replacement
- Emergency access to your SPHR

In order to validate this change, please activate the following URL:
http://www.esante.lu/notification_confirmations/63hg38937cfz3hjmz0b7wtz0gc

Figure 26: Email notification message

**Remarks:**

- There is really only one procedure for subscription and unsubscription. The system always presents the list of current subscriptions, which the user can change at will. Each modification requires a new confirmation by activation a URL specifically created for this action. The very first time a user connects to the notification service this list is empty, and no delivery email address is available.
- The user can enter one or more email addresses, separated by commas or semicolons. eSanté does not verify if all of these addresses are valid. However, it sends a confirmation email message with a unique activation URL to all of them. A change in the user's notification subscriptions is only accepted after the activation of this URL.

If there is more than one email address, every one of them has to activate the subscription in order to get notified. Moreover, adding or changing an email address is also considered a modification that has to be approved by the new email recipients, just like a new subscription. Removed recipients are not notified and simply do not receive notifications any longer.

# Glossary of terms

Wherever hyperlinks are provided in the text you can jump directly to the glossary entry with a simple click in the PDF document, or using Control + Click in MS-Word.

| Term | Description |
|---|---|
| **3rd Party Data Viewer** | Any person different from the patient, the prescriber and the lab biologist who validates the reports. Examples are:<br>• another general physician or specialist named by the patient, the prescriber or the original radiologist<br>• authorized medical emergency personnel |
| **Access rights** | (also called *access privileges* or *access control*)<br>They define which user has access to what data and services. Access can furthermore be refined in different types such as read (= view), write (= create, delete) modify, and so on.<br>**Examples:**<br>• Prescribers can view and copy data for exams they have prescribed.<br>• Radiologists can create, view, modify and delete their own radiology reports.<br>• Patients can view the reports of their own exams, but only after the prescriber or another authorized doctor, such as the reference doctor, has unblocked them.<br>Due to the lack of a proper patient consent management model at the time of writing of this document no specific roles and privileges can be given here. |
| **API, Web API** | An **Application Programming Interface (API)** is an interface implemented by a software program which enables it to interact with other software. It facilitates interaction between different software programs similar to the way the user interface facilitates interaction between humans and computers.[19]<br>A **Web API,** also sometimes called a **Web Service**, is typically defined as set of HTTP request messages along with a definition of the structure of response messages.[20] |
| **Authentication** | The act by which a physical person identifies him/herself to a computer system in order to gain entry into the system and access to its data. This is usually accomplished by using a login name and password, or more likely in this context, by using a secure token provided with a strong authentication method such as LuxTrust. |
| **Blocked data, read-block** | Most clinical documents sent to eSanté will be readable for the patient. However, the Data Provider can ask in the submission transaction that the report be "blocked" when submitting it to eSanté, meaning blocked for patient reading, while it remains readable for all authorized HCPs. The document itself can also be marked as blocked in its metadata. It stays blocked until the prescriber, the reference doctor or any other authorized HCP removes the block, usually during the so called *"visite d'annonce"*, so that the patient can |

[19] Definition from the Wikipedia, http://en.wikipedia.org/wiki/Application_programming_interface.
[20] Definition from the Wikipedia, http://en.wikipedia.org/wiki/Web_API

| Term | Description |
|---|---|
| | now read it. The patient himself can also remove the block if the HCP has given him the specific unblock code that was printed on the written report, or in the electronic version on eSanté. |
| **CDA, HL7 CDA r2** | The HL7 **Clinical Document Architecture** is an XML-based markup standard intended to specify the encoding, structure and semantics of clinical documents for exchange. It addresses features such as persistence, stewardship, potential for authentication, context, wholeness and human readability.<br>See http://en.wikipedia.org/wiki/Clinical_Document_Architecture for the full Wikipedia reference.<br>See e.g. the following Weblink for the normative reference: http://healthinfo.med.dal.ca/hl7intro/CDA_R2_normativewebedition/infrastructure/cda/cda.htm. |
| **Data Consumers, Data Recipients** | As opposed to Data Providers, the Consumers / Recipients are on the receiving side of the data flow. In the eSanté platform Data Consumers are securely identified physical persons who have access to patient data, such as prescribing physicians, reference doctors, and other 3rd party Data Consumers. Patients are a special case because the identification process in the eSanté platform is different for them, and they are therefore always called 'patients', rather than Data Consumers.<br>"Data Recipient" is essentially an equivalent term to "Data Consumer", which is preferred in transfer use cases, where medical data is explicitly "sent" to a limited number of recipients. The distinction is done to emphasis the transient character of the data transmission. |
| **Data Provider** | In eSanté a Data Provider is any participant who is allowed to submit data in the form of documents to the platform, for the purpose of sharing, exchange or both. All data providers must be uniquely identifiable by eSanté, otherwise they cannot submit documents. |
| **Data Provider Identification** | Data Providers are uniquely identified within eSanté. This is needed to<br>a) Deal with local patient IDs that are unique only within one Data Provider.<br>b) Identify the source of submitted documents.<br>Provider IDs are assigned by eSanté and do normally not change over time. Data Providers can submit data to eSanté only through secure nodes, which are securely authenticated by the eSanté platform in order to prevent unauthorized parties from submitting data. |
| **Data receiver centric View** | This term means that the Data Consumer is the pivotal point from which patient data is searched for. More specifically it means that the system shows data which have been explicitly sent to the consumer, and which may belong to any number of different patients. E.g. a prescriber can see all results to exams he has prescribed. This is in contrast to the patient centric view, where a user of the system can search for all accessible data for one given patient. |

| Term | Description |
|---|---|
| **Demographic Patient Data** | Usually the term "demographic" applies to all data that can be used to characterize a population. These types of data are used widely in sociology, public policy, and marketing. Commonly used demographics include gender, race, age, disabilities, mobility (in terms of travel time to work or number of vehicles available), home ownership, employment status, and even location.<br>eSanté deals only with part of these data, and its prime usage is the unique → identification of patients. A secondary usage is health statistics, which is more in line with the original meaning of the term "demographics". |
| **Document Registry** | The Document Registry is the storage area for document metadata in the eSanté platform. While the content of a document is stored in the Document Repository the metadata is kept in the Registry for querying. A search for documents is always carried out as a query on the Registry, never on the Repository.<br>See §3, Overall Framework for Data Transmission and Sharing, for more info and an example. |
| **Document Repository** | The document Repository is the storage area for document contents in the eSanté platform. Documents are composed of two parts: Metadata and content.[21] When documents are submitted to the Repository their metadata is separated from the content and registered in the Document Registry, while the document content is encrypted and stored in the Repository. Each Registry entry has a back-link to the document content entry in the Repository.<br>See §3, Overall Framework for Data Transmission and Sharing, for more info and an example. |
| **Document Type** | All documents in eSanté are typed according to an internal typing system. When submitting a document a valid type must be provided, otherwise the submission fails. In the case of eSanté-LABO the possible document types are[22]<br>• Partial Lab Report<br>• Complete Lab Report |
| **eSanté platform** | The overall IT system that delivers the services and functions described in this series of use cases. Its main purpose is to store medical data related to patients in the Luxemburgish health care system, and to facilitate the secure and controlled exchange of data among its different actors.<br>Beside data storage and transfer services the eSanté platform will provide other related services such as a Notification Service, the Patient Consent Management Service etc. |
| **GUI** | In computing a **Graphical User Interface** (GUI, sometimes pronounced gooey) is a type of user interface that allows users to interact with electronic devices with images rather than text commands. A GUI represents the information and actions available to a user through graphical icons and visual indicators such as secondary notation, as opposed to text-based interfaces, typed command |

[21] The exact format is specified in the CDA – Clinical Document Architecture.
[22] The actual type names in the formal CDA specification may be different. The present list is given for enumerating the different types that eSanté-LABO introduces.

| Term | Description |
|---|---|
| | labels or text navigation. The actions are usually performed through direct manipulation of the graphical elements.[23] |
| **HCP** | **Health Care Professionals** are professionals that work in the health care sector, such as doctors, nurses, midwifes, medical assistants, Samu, etc.<br>Each registered HCP has his own Incoming Folder in eSanté in order to be able to receive documents directly sent to him through the reliable transmission channel. |
| **HCP Registry** | Or **HCP Registry**. A component of the eSanté platform that represents a register of all HCPs that participate in the system. It provides registry and identification services for the HCPs working with eSanté. Only registered HCPs can access patient health care information from eSanté, and contribute own information to it. |
| **HCP software** | Software systems that are used by HCPs in order to conduct their work and manage their patients. Examples are<br>• Medical cabinet software,<br>• LIS / HIS / RIS / PACS<br>• Medical device software for monitoring patients<br>• ... |
| **Health Care Provider Identification** | In order to be able to participate and use the system a health care professional has to be registered in the eSanté platform. He is then given a unique HCP ID, which should be known and used by Data Providers to transmit data through reliable transmission.<br>The minimal set of information to identify uniquely a health care professional has still to be defined, but the following elements are good candidates :<br>• CNS-number<br>• Matricule<br>• A professional ID (not yet defined)<br>• Name and surname<br>• Medical specialty |
| **HIS** | **Hospital Information Systems** are comprehensive, integrated information systems designed to manage the medical, administrative, financial and legal aspects of a hospital and its service processing. Traditional approaches encompass paper-based information processing as well as resident work position and mobile data acquisition and presentation. |
| **IHE, IHE Profiles** | **Integrating the Healthcare Enterprise** (IHE), is a non-profit organization founded by healthcare professionals and the industry to improve the electronic information exchange in the healthcare sector.<br>**Integration Profiles** describe clinical information management use cases and specify how to use existing standards (HL7, DICOM, etc,...) to address them. Systems that implement integration profiles solve interoperability problems.<br>Systems that support IHE Integration Profiles work together better, are easier |

[23] Definition from Wikipedia, http://en.wikipedia.org/wiki/Graphical_user_interface.

| Term | Description |
|---|---|
| | to implement, and help care providers use information more effectively. The goal is efficient delivery of optimal patient care. Several hundred products support one or more IHE Profiles.<br>See the IHE Wiki Page at http://wiki.ihe.net/index.php?title=Main_Page for more information. |
| **Incoming Folder** | Sometimes also referred to as "Inbox", because of certain similarities with the Email system. Each HCP who is enrolled as a user in the eSanté platform has his own, private Inbox that only he himself can access. Patients can also be users of eSanté, but do not have an Inbox[24].<br>The Inbox serves as a temporary storage for documents delivered through the reliable transmission channel. See chapter §2 Architectural Considerations.<br>HCPs connected to eSanté can see the content of their Inbox and download all documents contained in it. Once downloaded the documents are removed, similar to the download-and-delete mode of the Post Office Protocol (POP) for email delivery. |
| **Lab Report** | Laboratory Test Reports (or short: Lab Reports) submitted to the eSanté platform have to respect the HL7-CDA r2 format.<br>They can be structured (i.e. completely expressed in XML) or unstructured (PDF embedded in an XML frame). Charts, graphics, etc., can be embedded in the report, but are limited to small images in gif, jpeg, png or bmp format, and must be encoded in Base 64. The syntactic format of such a lab report, i.e. the precise XML structure, is described in IHE LAB TF-3 Content, Chapter 2.3 Specification. The semantic content, and especially the choice of code systems that should be used, have to be defined and agreed upon by a inter-laboratory workgroup such as the LABO-LOINC group. |
| **Laboratory data,**<br>**Partial results,**<br>**Complete report** | Refers to laboratory test results, for which we distinguish 2 types<br>• **Partial results** – a subset of the results that have been ordered<br>• **Complete report** – the whole set of ordered results<br>Often a prescriber orders a series of tests in relation with a certain clinical situation of his patient. The lab breaks down the entire order into individual tests. Depending on the nature of the tests and the lab's internal workflow these results may become available at different moments in time, and therefore be published or sent out to the prescriber in more than one report, as so called ***partial results or reports***. After the last test is done the lab assembles all partial results into a ***complete report***.<br>All partial results build up to the final complete report. Example: a test order is split into 3 parts: A, B and C. The 1st report contains test results A, the 2nd A + B, and the 3rd (= complete report) contains results A + B + C.<br>It is current practice that patients receive only complete reports, while doctors get both partial and complete reports.<br>Other information about the report such as the date of creation, a subject/title, the type of tests it contains, the name of the validating biologist |

[24] At least not in the first version of the platform.

| Term | Description |
|---|---|
| | etc. is called meta information. |
| **LIS** | A **Laboratory Information System** (LIS) is a class of software that receives, processes, and stores information generated by medical laboratory processes. These systems often must interface with instruments and other information systems such as Hospital Information Systems (HIS).<br>Most Luxemburgish laboratories use GLIMPS (General Laboratory InforMation System), from the Belgian software editor MIPS. The same company also provides the Laboratory Web visualization solution **Cyberlab**. |
| **Longitudinal Record** | This expression is sometimes used to refer to the SPHR. A SPHR can be seen as a set of documents, residing in the registry and the repository, being aligned in chronological order and referring all to the same patient.<br>The expression originates from the medical context, where a longitudinal study is a correlational research study that involves repeated observations of the same items over long periods of time. The order criterion for the longitudinal record is time.<br>In contrast to the longitudinal record is the so called case record, which represents a subset of the longitudinal record, by grouping together related documents that are relevant to a specific aspect of the patient's health care, e.g. for a patient referral.<br>See §2, Architectural Considerations, for an example. |
| **Metadata** | Or *Meta-Information*. A document is composed of two kinds of information:<br>• actual lab report data, which are also called *document content*, and<br>• metadata, e.g. the patient, date and time of creation, Title, short description, modality, author, etc.<br>Metadata is very useful for searching documents. Typically a user will query the Document Registry for matching metadata, then he can retrieve the document content from the Document Repository. |
| **MPI** | Short for **Master Patient Index**.<br>Wikipedia defines it as follows (German version):<br>*Der Master Patient Index (MPI) ist ein Konzept zur Überwindung der Schranken zwischen Krankenhaus-IT-Lösungen verschiedener Hersteller oder Generationen ohne Gefährdung des Patienten. Dazu wird im MPI ein Index verwaltet, welcher möglichst alle bekannten und vergebenen Identitäten und Indices eines Patienten aus verschiedenen Bereichen (Krankenhäusern, Abteilungen eines Krankenhauses, Arztpraxen etc.) referieren soll. Ein MPI dient dazu, die Information aus den verschiedenen Quellen unter einer gemeinsamen Identität (einem Index) auch übergreifend über aufeinanderfolgende Fälle desselben Patienten aufzufinden.*<br>eSanté offers MPI functionality as an extension of its Patient Registry, by federating local patient identification and demographic information from various sources in a central registry. E.g. local patient IDs coming from different Data Providers can be associated with one and the same patient, if |

| Term | Description |
|---|---|
| | sufficient demographic patient identification was provided to guarantee a unique match.<br><br>The high security standards of eSanté require that demographic patient information and medical data be strictly separated from each other, which also applies to the MPI. Therefore the MPI is implemented as a service of the TTP, which achieves the security goals by means of de-identification and pseudonymisation. |
| **Notification Service** | Sub-system of the eSanté platform that can be used to subscribe / unsubscribe to a notification service. This service automatically generates messages at specific events, such as the availability of new radiology exam data, or access to a patient's medical record. |
| **Opt-in, opt-out** | These are basic options for the participation of patients in the consent management process.<br>Opt-in means that patients by default have not given consent to participate in the eSanté platform, and therefore explicitly need to declare their consent in order to participate.<br>Opt-out means participation by default (consent given), unless consent is explicitly revoked.<br>At that point it can be assumed rather safely that all persons being registered with the CNS will be enrolled on an opt-out basis, while other persons coming in contact with the Luxemburgish Health system are managed on an opt-in basis.<br>The Luxemburgish law on the Dossier de Soin Partagé (DSP) stipulates the opt-out option for patient consent. |
| **Parent Document** | CDA documents can be linked among each other by so called **Parent Document Links**. This linkage mechanism is independent from any XDS Registry/Repository infrastructure and operates only at document level. Therefore it is particularly well suited for linking documents that are exchanged over an XDR scenario.<br><br>However, contrary to the XDS case, where document references are kept in the Registry, and thus can be validated for correct document referral, the CDA document links cannot be guaranteed to point to existing documents.<br><br>HL7 CDA r2 imposes type restrictions and other constraints on the usage of inter-document links:<br><br>"A conformant CDA document can have a single relatedDocument with typeCode "APND"; a single relatedDocument with typeCode "RPLC"; a single relatedDocument with typeCode "XFRM"; a combination of two relatedDocuments with typeCodes "XFRM" and "RPLC"; or a combination of two relatedDocuments with typeCodes "XFRM" and "APND". No other combinations are allowed." |
| **Patient Centric View** | This means that the patient is the pivotal point from which patient data is searched for. It specifically means that one search operation can only return data for one given patient. This is in contrast to the consumer centric view, |

| Term | Description |
|---|---|
| | where a Data Consumer such as the prescriber can search for results he is the consumer of, no matter for which patient. |
| **Patient Consent Management** | Or shortly **Consent Management**. A system of roles and rules that allows a patient to define the access conditions to his SPHR on the eSanté platform. Wikipedia describes its functions as follows:<br>Consent management is a system, process or set of policies for allowing consumers and patients to determine what health information they are willing to permit their various care providers to access. It enables patients and consumers to affirm their participation in e-health initiatives and to establish privacy preferences to determine who will have access to their protected health information (PHI), for what purpose and under what circumstances. Consent management supports the dynamic creation, management and enforcement of consumer, organizational and jurisdictional privacy directives. |
| **Patient Identification Information** | In eSanté patients are identified by the Patient Registry, which itself is implemented as a service of the TTP. The following non exhaustive list of attributes is used to identify patients:<br>Name, surname, maiden name, gender, birth date, matricule or other social security number (SSN), nationalities, birth place, address(es), local patient ID in the Data Provider's system, provider ID (useful in combination with the patient local ID).<br>The Patient Registry can be queried using these attributes, in order to return references that can be used to link individual documents with the patients. |
| **Patient Registry** | The Patient Registry is an eSanté service of the TTP that manages all patients known to eSanté. It receives the major part of its patient information from the various Data Providers, but other sources like a national person register are also possible as data input.<br>The Patient Registry can be queried with Patient Identification Information in order to obtain a match. Because of security reasons it returns only pseudonyms that could be used to associate medical records directly with patients. Those pseudonyms are used in the Document Registry to provide anonymous references to a patient without ever revealing his actual identity. |
| **PMS** | A **Patient Management System** is a Health Care Professional Software that supports a HCP in managing his patients. Those systems have usually a database containing both administrative/demographic and medical information about the doctor's patients. Other functions such as billing, letter generation, agenda and waiting room management often complete the PMS to a ***Medical Cabinet Management System***.<br>Most PMS can store and associate arbitrary files to a patient's record, such as lab reports, radiology images & reports, letters, other pictures etc. |
| **PACS** | **Picture Archiving and Communication System**, is used in the healthcare sector mainly as an electronic archive for the storage and retrieval of digital images from multiple modalities (source machine types), e.g. CT and MR.<br>Electronic images and reports are transmitted digitally via PACS; this |

| Term | Description |
|---|---|
| | eliminates the need to manually file, retrieve, or transport film jackets. |
| **Positive & negative consent situation** | A patient is said to have a positive consent situation if he has agreed to have his medical data permanently stored in eSanté, i.e. he agrees to have a SPHR. A negative consent situation means the opposite, i.e. a patient does not agree to have his medical data stored permanently in eSanté. As a consequence, patients with positive consent (and their HCPs) can use eSanté's data sharing services related to the patient's data, patients with negative consent can't. |
| **Prescriber** | (also sometimes called *prescribing physician*) is, in the context of LABO, a doctor who has prescribed a laboratory exam to his patient. It is, however, not a formal role in the LABO use cases. What is important about the prescriber is that he receives the results of his exam prescriptions, and therefore the use cases rather calls him the Data Consumer/recipient.<br>There is also the concept of the reference doctor, which is in most of the cases also the prescriber of an exam. But this doctor has other functions that go beyond making prescriptions. |
| **Reference Doctor** | A general physician who has a special trust relationship with a patient. In the eSanté platform the reference doctor has special privileges and functions in respect with his patients' medical data such as:<br>• having a privileged access to his patient's medical data record<br>• to unblock critical data so that the patient can see them[25]<br>• sharing his patient's medical data with other HCPs in agreement with the patient<br>He also happens to be the principal prescriber of most of the patient's exams.<br>The reference doctor will occupy a key position in the Luxemburgish health system. He will sign a contract with the patient and the government (CNS) that puts him in charge of the |
| **RIS** | A **Radiology Information System** is a computerized database used by radiology departments to store, manipulate and distribute patient radiological data and imagery. The system generally consists of patient tracking and scheduling, result reporting and image tracking capabilities. RIS complements HIS and is critical to efficient workflow to radiology practices. |
| **Secure Node** | A secure node is a software system that interacts with eSanté by means of certain transactions, e.g. data submission. Secure nodes are required to use strong authentication to connect to eSanté. Logins on secure nodes are implicitly trusted be eSanté to be secure in turn, so that no further authentication of secure node users vis-à-vis eSanté is required.<br>E.g. if a lab's LIS system is a secure node the lab personnel working on it do not have to be authenticated vis-à-vis eSanté. If there is one eSanté connector for a hospital all subsystems that log into that connector (HIS, LIS, RIS, PACS, ...) and their respective users are implicitly trusted to be secure.<br>Secure nodes maintain a list of uniquely identified Data Providers that are allowed to submit data through the node. |

[25] This function is not limited to the reference doctor.

| Term | Description |
|---|---|
| **SPHR** | A SPHR or **Shared Patient Health Record** is an electronic health record for individuals that is located on the eSanté platform, and which can be viewed by anyone who has the necessary electronic credentials to access this information.<br>An ideal SPHR would provide a complete and accurate summary of the health and medical history of a person by gathering data from many sources. |
| **Test Validation** | Today it is common practice and also a quality requirement that laboratories validate test results in a three-step process:<br>1. ***automatic validation*** by the test equipment and its controlling software<br>2. ***technical validation*** by a lab technician<br>3. ***clinical validation*** by the responsible lab biologist<br>The publishing of results largely depends on these states of validation, but can be different depending on the lab. A lab hospital e.g. may publish technically validated results to services within the hospital, but only clinically validated results outside the hospital. Private labs in general would only publish clinically validated results. Tests that are only automatically validated should never be made available outside the laboratory. |
| **TTP** | The **Trusted Third Party** is a system that offers a number of security related services and functions to the eSanté platform such as:<br>• Secure Patient Registry, which holds the registry of all patients known to eSanté.<br>• Master Patient Index, an extension of the Patient Registry service which allows that patient identification data sets from multiple sources can be matched with one and the same patient.<br>• De-identification and pseudonymisation.<br>Instead of returning a unique ID for a patient match, the TTP produces and returns pseudonyms when queried with valid patient identification information.<br>• Key management for document encryption.<br>The TTP provides public key certificates that are used in the document encryption process. |
| **Unblock Code and Function** | Documents submitted to the eSanté can be marked as unreadable for the patient (read-block). There is a user function that allows the patient himself to unblock a document that is otherwise blocked to him from reading. The idea is that a doctor, who uses eSanté rarely or not at all, can enable the patient to unblock the document himself, by giving him the necessary unblocking code.<br>To make this possible the Data Provider should arrange to print a code composed of numbers and letters on any version of the document he distributes to the doctor through his own channels (paper, Web, iPhone…). It should also be present in the electronic document's metadata set that he sends to eSanté. Only HCPs will receive documents containing this code.<br>If the patient is given this code by a doctor who has access to the document, |

| Term | Description |
|---|---|
| | the patient can then use it to unblock the document himself, thereby gaining permanent access to it. |
| **UUID** | **Universally Unique Identifiers** are system-generated IDs that guarantee practical uniqueness[26] across decentralized systems.<br>The intent of UUIDs is to enable distributed systems to uniquely identify information without significant central coordination. Thus, anyone can create a UUID and use it to identify something with reasonable confidence that the identifier will never be unintentionally used by anyone for anything else. Information labeled with UUIDs can therefore be later combined into a single database without needing to resolve name conflicts.<br>See http://en.wikipedia.org/wiki/Universally_unique_identifier for the full article and http://www.ihe.net/Technical_Framework/upload/IHE_ITI_TF_6-0_Vol3_FT_2009-08-10-2.pdf p. 33 for a IHE relevant example. |
| **XDR** | Short for **Cross-Enterprise Document Reliable Interchange**. XDR is a IHE profile that provides document interchange using a reliable messaging system. This allows for direct document interchange between healthcare IT systems in the absence of a permanent document sharing infrastructure such as XDS.<br>In the case of eSanté XDR will be implemented using the XDS infrastructure (Registry, Repository)<br>See http://wiki.ihe.net/index.php?title=XDR and http://www.ihe.net/Technical_Framework/upload/IHE_ITI_TF_Rev7-0_Vol1_FT_2010-08-10.pdf, p. 125 -127 for more details. |
| **XDS** | Short for **Cross-Enterprise Document Sharing.** XDS is a IHE profile that focuses on providing a standards-based specification for managing the sharing of documents between any healthcare enterprise, ranging from a private physician office to a clinic to an acute care in-patient facility and personal health record systems. This is managed through federated document repositories and a document registry to create a longitudinal record of information about a patient within a given clinical affinity domain.<br>See http://wiki.ihe.net/index.php?title=Cross-Enterprise_Document_Sharing and http://www.ihe.net/Technical_Framework/upload/IHE_ITI_TF_Rev7-0_Vol1_FT_2010-08-10.pdf, p. 69 - 99 for more details. |

[26] In contrast to theoretical uniqueness, which cannot be claimed because of the technical length limitation of a UUID (usually 16 byte = 128 bit).

# References to other documents

| Reference | Title | Author | Version/Date |
|---|---|---|---|
| **eSante Architecture WP7 and WP8** | Project eSante Architecture and Security of a National eHealth Platform (Deliverable for WP7, WP8, WP13) | CRP Henri Tudor, SANTEC | Version 1.06 29/6/2011 |
| **LABO WP5 CDC Technique**<br>**CARA2 WP13 CDC Technique** | Cahier des charges techniques General Requirements Document<br><br>(one deliverable for two projects, therefore two references, for now) | CRP Henri Tudor, SANTEC | Version 0.3 4/10/2011 |
| **IHE Lab TF-3 Vol3** | IHE Laboratory (LAB) Technical Framework Volume 3 (LAB TF-3) Content | IHE International, Inc. | Revision 3.0 – Final Text 20 May 19, 2011 |