Title:	*Evaluation Report*
Author:	*Work Package 8 ("Application 2: organ transplant management")*
Editor:	*Javier Vázquez-Salceda and Sergio Álvarez (UPC), László Zs. Varga and Kifor Tamás (MTA SZTAKI)*
Reviewers:	*All project partners involved*
Identifier:	*D8.2.1*
Type:	*Deliverable*
Version:	*v1.0*
Date:	*November 30th , 2006*
Status:	*Final*
Class:	*Public*

Summary

This document presents the evaluation of the demonstration applications in Work Package 8 *"Application 2: organ transplant management"*.

The PROVENANCE project receives research funding from the European Community's Sixth Framework Programme

Members of the PROVENANCE Consortium:

IBM United Kingdom Limited	United Kingdom
University of Southampton	United Kingdom
University of Wales, Cardiff	United Kingdom
Deutsches Zentrum für Luft- und Raumfahrt e. V.	Germany
Universitat Politecnica de Catalunya	Spain
Magyar Tudomanyos Akademia Szamitastechnikai es Automatizalasi Kutato Intezet	Hungary

Foreword

The purpose of this document is to provide an evaluation for the demonstration application in the organ transplant scenario.

The document provides:

a. a summary of the user requirements and software requirements coming from the requirement capture in WP2 that are related to the organ transplant scenario;

b. an evaluation on how these requirements are fulfilled by the implemented application, identifying the part of the application, the provenance architecture or the tools responsible for each requirement;

c. a description of the test scenarios that have been used to make a functional evaluation of the demonstration applications;

d. the results of the evaluation made by potential users over the demonstration application.

The primary audience of this document includes: A) Grid computing practitioners seeking to understand how Provenance technologies might be applied and, B) Information technology practitioners in the health care domain interested in applying Provenance to their own medical systems.

Table of Contents

List of Acronyms

Acronym	*Description*
AR	Abstract level capability user requirements
CR	Constraint user requirements
DNI	Spanish National Identity Number
EHCR	Electronic Health Care Record
EHCRS	Electronic Health Care Record Store
GMPID	Global Medical Patient Identifier
GP	General Practitioner
GUI	Graphical User Interface.
HCR	Health Care Record
HLA	Human Leukocyte Antigens test
IT	Information Technology
LMPID	Local Medical Patient Identifier
OCATT	Organització Catalana de Transplantaments (Catalan Transplant Organisation)
ONT	Organización Nacional de Transplantes (Spanish National Transplant Organisation)
OTA	Organ Transplant Authority
OTM	Organ Transplant Management
PDF	Portable Document Format, Adobe Inc.
PID	Patient Identifier
PS	Provenance Store
SR	Software Requirements
TR	Technical level capability user requirements

1 Introduction

This document presents the evaluation of the demonstration applications in Work Package 8 *"Application 2: organ transplant management"*. This document provides an evaluation in terms of:

- fulfillment of the user and software requirements specified in Workpàckage 2,
- evaluation provided by potential users of the system.

The primary audience of this document includes: A) Grid computing practitioners seeking to understand how Provenance technologies might be applied and, B) Information technology practitioners in the health care domain interested in applying Provenance to their own medical systems.

1.1 Purpose of the Document and Overview

The purpose of the document is to provide a careful evaluation for the demonstration application in the organ transplant scenario. This application is composed by two inter-connected applications: the Organ Transplant Management application (OTM) and the Electronic Health Care Record System application (EHCRS). Secondary goals include:

- Evaluating the fulfillment of the expected benefits of introducing provenance in both OTM and EHCRS applications
- Reporting the opinions users have provided over the new functionalities in both OTM and EHCRS by introducing provenance.

In order to achieve these goals, the document aims to:

- Summarize the user requirements and software requirements coming from the requirements captured in WP2 that are related to the organ transplant scenario.
- Evaluate the fulfillment of the aforementioned requirements in the implemented application, identifying the part of the application, the provenance architecture or the tools responsible for each requirement.
- Describe the test scenarios that have been used to make a functional evaluation of the demonstration applications.
- Present the results of the evaluation made by potential users over the demonstration application.

.

This document does not aim to:

- Describe in full detail the organ transplant scenario, the OTM and EHCRS applications. The reader interested in this can find more details in Deliverables D8.1.1. and D8.3.1.
- Evaluate all the functionalities of OTM and EHCRS that are not related to provenance issues. Evaluation will be centered only in those aspects of the application that are related to the introduction of provenance.
- Provide a description on how provenance has been introduced in OTM and EHCRS. The reader interested in this aspect can find more details in Deliverables D8.1.1. and D8.3.1.

1.2 Links to other Provenance Documents

The contents of this document are based on the following existing Provenance project documents:

- Requirements expressed for the OTM application in the WP2 Requirements deliverables D2.1.1 and D2.2.1.
- The Provenance architecture document D3.1.1.
- Project internal note on "Representing Provenance in the OTM application" [Miles05].
- Deliverable D8.1.1. "Specification of mapping to provenance architecture, and domain specific provenance handling "
- Deliverable D8.3.1. "Final deployment"

Further supporting documents are provided in the references section.

1.3 Short description of the OTM and EHCRS applications

Electronic systems for transplant management should cover 2 aspects:

1. *Transplantation Management*: information systems used by medical staff during the process of a transplant incident (a single patient receiving an organ or tissue) to access existing case or background data, share it with colleagues, carry out matchmaking and/or otherwise provide decision support.

2. *Medical Record management*: the storage, access and modification of medical patient care records for patients in a given geographic region. Gathering, access and modification of such data is regulated by European, national and regional laws and forms an underlying information system for any treatment process management system.

Therefore the demonstration application developed in Work Package 8 is actually composed of two interconnected applications:
- transplant management is provided by the Organ Transplant Management (OTM) application,
- medical record management is provided by the Electronic Health Care Record (EHCRS) application.

Although in this document we will refer to each of these applications separately, both function together and can be seen from the user perspective as a single application, with the OTM application directly accessing and making use of the EHCRS functionality.

Following subsections present a short description of each of the applications.

1.3.1 Transplantation Management and Post-processing: The OTM Application

The Organ Transplant Management (OTM) Application aims to speed up the allocation process of solid organs to improve graft survival rates. Its policy implements the Spanish guidelines for organ and tissue procurement and Spanish regulations for allocation, as Spain is world leader in the area, followed as a model by other countries. OTM uses standard web service technology and has been adapted to be provenance-aware, by interacting with the provenance stores in order to keep track of the distributed execution of the allocation process for audit purposes.
Figure 1 summarizes the different administrative domains (solid boxes) and units (dashed boxes) that are modelled in the OTM application. Each of these interact with each other through Web Service

interfaces (circles) that send or receive messages. The Organ Transplant Authority (OTA) is an administrative domain with no internal units. In a transplantation management scenario, one or more hospital units may be involved: the hospital transplant unit, one or several units that provide laboratory tests and the unit that is responsible for the patient records (which will use the EHCRS application services, see section 1.3.2). The diagram also shows some of the data stores that are involved: apart of the patient records, these include stores for the transplant units and the OTA recipient waiting lists (WL). Hospitals that are the origin of a donation also keep records of the donations performed, while hospitals that are recipients of the donation may include such information in the recipient's patient record. The OTA has its own records of each donation, stored case by case.

More specifically, Figure 1 also shows an example of a typical interaction between these actors: a transplant management scenario starts with a potential donor in Hospital A's transplant unit. In order to evaluate the donor, this unit may request the patient records inside the hospital and order a number of tests, some of them to internal laboratory units and others to some specialized external laboratories. Once the donor is evaluated and, if valid, the transplant unit contacts the OTA, which sends first the offer to hospital C. As the transplant unit in hospital C rejects the donation, the OTA sends the offer to hospital B, which has a potential recipient for the organ offer (as in the case of Hospital A, all the medical data needed for the recipient was previously collected by hospital B by interacting with the ECHRS application and the testing laboratories). During extraction and implantation, direct communication between hospital A and hospital B and also between the OTA and the hospitals occurs.

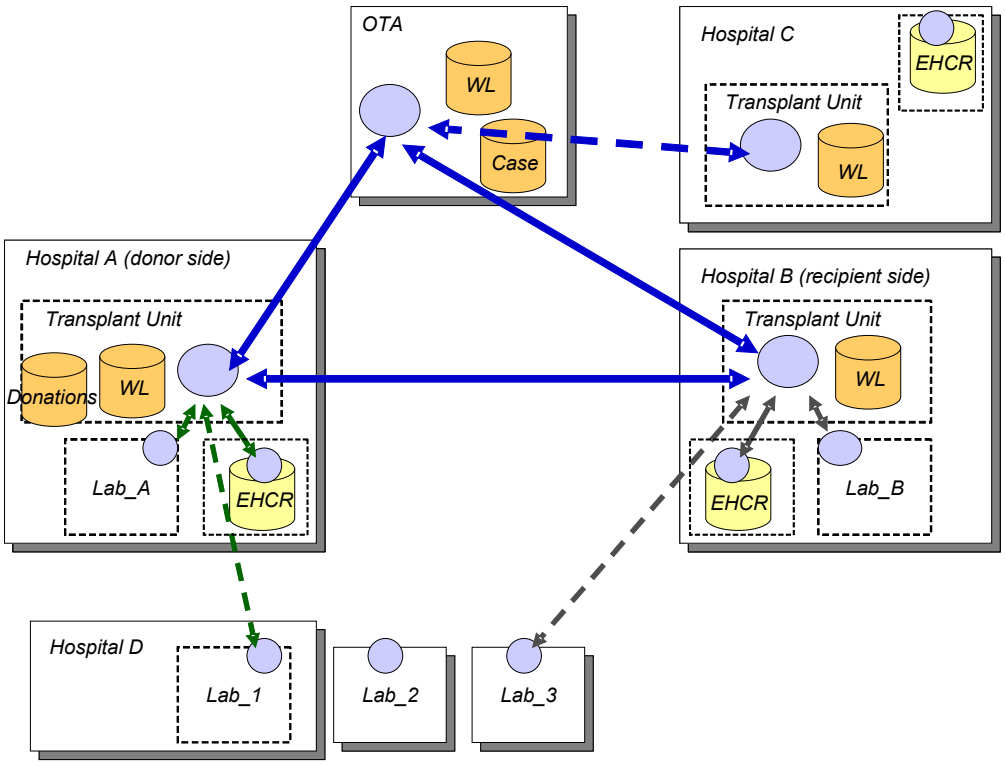


Figure 1 -- Actors in the OTM application.

By transforming OTM into a *provenance-aware* application, OTM is augmented with a capability to produce at run-time an explicit representation of the process actually taking place (examples can be seen in section B.2.3 and B.3.3). Such representation can be then queried and analysed in order to extract valuable information to validate, e.g., the decisions taken in a given case, or to make an audit of the system over a period of time.

1.3.2 The EHCRS Application

The Electronic Health Care Record Store Application (EHCRS) provides a way to manage electronic health records distributed in different institutions. The architecture provides the structures to build a part of or the entire patient's healthcare record drawn from any number of heterogeneous databases systems in order to exchange it with other healthcare information systems.

The EHCRS architecture provides a Web Service interface that receives and sends messages (following ENV13606 pre-standard format [ENV13606]) for local and remote medical applications. The EHCRS application also uses an authentication Web Service to authorize request messages from remote health care parties.

The EHCRS application is used by the OTM application as its primary store of patient care data. But it is important to note that the EHCRS application was intended to be not only the application to store medical records for the needs of the OTM application, but a generic system for storing and collating health care records across multiple health care providers, usable by other health care grid applications.

Making the EHCRS system *provenance-aware* provides a way to have a unified view of a patient's medical record with its provenance (i.e. to connect each part of the medical record with the processes in the real world that originated it and/or the individuals, teams or units responsible for each piece of data).

1.4 Summary

In summary, the OTM application is divided into two parts: an underlying health care record management element and the OTM application itself. These two applications are seen by the user as a single application that provides both the transplantation management and the medical record management integrated in OTM's user interface.

2 Technical Evaluation

In this chapter a technical evaluation of the OTM and EHCRS applications is provided. This evaluation is based in the analysis of the fulfillment of the requirements identified in Work Package 2.

It is important to note that in this chapter and in the next chapter we will center our evaluation in the functional and non-functional aspects of OTM and EHCRS that are related with provenance. Full evaluation of functionalities and user requirements in both OTM and EHCRS will be provided in the CARREL@FIS project.

The design and implementation process of making both OTM and EHCRS applications provenance-aware was based in the technical requirements on the provenance architecture that were documented in the Software Requirements Document [D2.2.1]. The determination of these technical requirements was based on the analysis of the User Requirements Document [D2.1.1] carried out in Work Package 2. by the software architects and developers of the project team. However, the software requirements in [D2.2.1] are more focused on requirements for the provenance architecture, the client-side libraries, and the tools, and were abstracted from the applications.

Therefore, in the following sections we will base our evaluation of requirements' fulfillment not only in the technical requirements in [D2.2.1], but also in the analysis of fulfillment with the original user requirements on [D2.1.1].

Presentation is divided into 2 major sections: in section 2.1 we will first go through the user requirements to evaluate the system from the user point of view. Then in section 2.2 we will evaluate the extent that OTM and EHCRS contribute in the technical requirements' fulfillment.

2.1 Fulfillment of User Requirements

In this section we will analyze the fulfillment of the user requirements in [D2.1.1] that were related with the organ transplant management scenario.

A summary of the user requirements relevant for the organ transplant scenario is available in Appendix A1.

2.1.1 Abstract level capability user requirements

Abstract level capability user requirements described in detail what users wanted to use provenance for in their application scenarios. They are mainly related to provenance questions which might be asked during or after the operation of the EHCRS subsystem.

2.1.1.1 Domain specific provenance questions:

(These questions can only be answered by processing domain specific content in recorded data.)

AR-1-1: The provenance system should support the following operation:

Check a given set of decisions in a case against the established rules to ensure that it is conformant. These rules may or may not be automatically enforced by the transplant management software – however in the general case many of them will not be. This provenance question is a post-hoc check as to whether rules were followed.

Requirement applies to: OTM
Accepted requirement: yes
If rejected, then reason: -
Deployed implementation feature: Rules have been expressed following JESS format.

These rules can be imported into the Rule Analysis tool. OTM can then use the Rule Analysis tool to check if the recorded decisions and steps in the process follow the rules. Internally OTM also makes some automatic enforcement of the rules, although allows some flexibility in some cases (e.g. to allow requesting a test without all the pre-conditions holding, for emergency purposes).

AR-1-2: The provenance system should support the following operation:

Derive a trace of the arguments, contributing factors and intermediate results which lead to a particular decision. (asked by Transplant Authority, Families, 3rd parties, Physicians)

Requirement applies to: OTM, EHCRS
Accepted requirement: yes
If rejected, then reason: -
Deployed implementation feature: Both OTM and EHCRS record the p-assertions related to the different steps of the transplant management, retrieval of patient records used in the arguments, contributing factors and intermediate results which lead to a particular decision. These p-assertions can be used to derive a trace.

AR-1-3: The provenance system should support the following operation:

Derive aggregate information across many cases such as the percentage of incidents of a certain type, success rates by center, etc. (asked by Transplant Authority, researchers, physicians)

Requirement applies to: OTM, EHCRS
Accepted requirement: yes
If rejected, then reason: -
Deployed implementation feature: Both OTM and EHCRS record p-assertions related to all cases. Based on these p-assertions, OTM can extract aggregate information by means of queries requesting this aggregate information.

AR-1-4: (optional) As an advanced feature the provenance system could support the following operation:

Truth maintenance for "next best candidate" or other dynamic information. Advanced functionality: meaning that the system could be used to keep up to date pre-calculated lists of recipients ready for an incident. This is a type of result which may need to be modified as underlying data changes. (asked by transplant system itself, physicians)

Requirement applies to: OTM
Accepted requirement: partially
If rejected, then reason:
Deployed implementation feature: the OTM system keeps updated recipient waiting lists. The "next best candidate" functionality was implemented in first versions of the OTM prototype. However an intermediate user evaluation of this functionality showed that it was hard to automate it, as best candidate is a decision involving not only a huge combination of medical conditions and exceptional cases but also by other factors such as the candidate already present in the hospital, the feasibility to contact with him in a fast way and the time the patient would need to arrive to the hospital.

2.1.1.2 Generic provenance questions:

(These questions can only be answered with derivations (reasoning) of some kind over recorded data but not using domain specific content.)

AR-1-5: The provenance system should support the following operation:

Extraction of an entire case-trace: gather all the records related to one incident into a single case-file. (asked by physicians, families, patients)

Requirement applies to: OTM, EHCRS
Accepted requirement: partially

If rejected, then reason: -
Deployed implementation feature: Both OTM and EHCRS record p-assertions related to all cases. The entire case trace can then be visualized through the Provenance Trace Portlet. The functionality to export all this data to an external file was dropped as it creates a huge personal data protection risk: if all this information is exported outside the system it is impossible to control further use compliance to security and privacy policies.

AR-1-6: The provenance system should support the following operation:
Identify all individual users related to an incident. (asked by physicians, Organ Transplant Authority, 3rd parties (legal challenges))

Requirement applies to: OTM, EHCRS
Accepted requirement: yes
If rejected, then reason: -
Deployed implementation feature: All users should log into OTM. The EHCR_Auth service of the EHCRS subsystem authorizes all users in the OTM application. All the interactions with the EHCR_Auth service are recorded in the Provenance Store. Based on the p-assertion of these interactions the identity of the users related to an incident can be retrieved from the original medical application.

AR-1-7: The provenance system should support the following operation:
Replay service execution flow/verify this against template workflows and/or rules governing procedures (Sophistication may vary). (asked by physicians, organ transplant authority, 3rd parties (legal challenges))

Requirement applies to: OTM
Accepted requirement: yes
If rejected, then reason: -
Deployed implementation feature: Procedural rules have been expressed following JESS format. These rules can be imported into the Rule Analysis tool. OTM can then use the Rule Analysis tool to check if the recorded decisions and steps in the process follow the rules.

AR-1-8: As an advanced feature the provenance system could support the following operation:
Identify abstract derivation process of the result – based on some shared high level notions of the types of actions/content logged (e.g. having a standard view of what is an assertion, what is a decision etc.) and what follows what.

Requirement applies to: OTM, EHCRS
Accepted requirement: yes
If rejected, then reason:
Deployed implementation feature: Both OTM and EHCRS record p-assertions related to all cases in several abstraction levels (from low-level step-by-step recording to high-level recording). By means of queries targeting the higher level p-assertions, the user can see in the Provenance Trace Portlet higher level traces of the process.

2.1.2 Technical level capability user requirements

2.1.2.1 Characteristics of provenance data

It is expected that automated logging mechanisms for the transplant application need to record the following raw data and information:

TR-1-1-A-1: Recording of the following provenance information is required:
Service invocation: Who accessed a particular service, when, with what input parameters (or a summary thereof) and on whose authority.

Requirement applies to: OTM, EHCRS
Accepted requirement: yes
If rejected, then reason: -
Deployed implementation feature: Both OTM and EHCRS record in p-assertions who accessed a particular service, when and with what input parameters. The authority information is recorded by the EHCR_Auth service.

TR-1-1-A-2: Recording of the following provenance information is required:
Service response: Who a service sent data messages to, in response to which invocation, the content of the response (or a summary thereof).

Requirement applies to: OTM, EHCRS
Accepted requirement: yes
If rejected, then reason: -
Deployed implementation feature: Both OTM and EHCRS record in interaction p-assertions who the data message is sent to. They also record in relationship p-assertions in response to which invocation the data message is sent to.

TR-1-1-A-3: Recording of the following provenance information would be useful:
Information state: A summary of the information state in the service at the time a particular action is taken.

Requirement applies to: OTM, EHCRS
Accepted requirement: yes
If rejected, then reason: -
Deployed implementation feature: Both OTM and EHCRS subsystem record in actor state p-assertion some relevant states of services at the time a particular action is taken.

TR-1-1-A-4: In addition to the logging of message based activities the provenance service also needs to capture "side effect" type actions submitted by the application (e.g. those which may not directly lead to a response message):

1. Carrying out an action in the real world
2. Recording a decision or fact

Requirement applies to: OTM, EHCRS
Accepted requirement: yes
If rejected, then reason: -
Deployed implementation feature: All relevant actions that are carried out inside both OTM and EHCRS are recorded in the form of p-assertions. In the case of actions performed in the real world (such as decisions, reports and factual observations) are entered by the user into the user interface of the OTM application. If they are relevant for the patient record, then they are also sent to the EHCRS subsystem. Both OTM and EHCRS record these actions by p-assertions and the data related to the "side effect" type of actions can be retrieved later from the OTM application.

2.1.2.2 Export and API format of provenance data

Requirements imposed on this issue by the individual applications:

TR-2-1-A: "Format must be a non-proprietary format which can in principle be used with another tool (to be built if necessary) without violating IPR rules. An open standard would be best."

Requirement applies to: OTM (indirectly), EHCRS (indirectly)
Accepted requirement: yes
If rejected, then reason: -
Deployed implementation feature: The provenance data format has been established

by the provenance architecture in Work Package 3. This format is non-proprietary and is used by both OTM and EHCRS to record p-assertions.

2.1.2.3 Storage and export of provenance data

TR-3-2: The system should support the recording of different views on provenance information regarding to an event or an entity.

Requirement applies to: OTM, EHCRS
Accepted requirement: yes
If rejected, then reason: -
Deployed implementation feature: The EHCRS subsystem records interaction, relationship and state p-assertions in order to support the recording of different views on provenance information regarding to an event or an entity.

TR-3-3: The system should support the migration of provenance data among provenance repositories.

Requirement applies to: OTM (marginally), EHCRS (marginally)
Accepted requirement: yes
If rejected, then reason: -
Deployed implementation feature: The provenance data recorded by OTM and EHCRS can be migrated among provenance repositories by export and import functions in the EXIST interface.

TR-3-4-A: On the fly recording of provenance data should be supported by the system.

Requirement applies to: OTM, EHCRS
Accepted requirement: yes
If rejected, then reason: -
Deployed implementation feature: The internal architecture of OTM and EHCRS makes a separation between the execution of the system and the asynchronous recording of provenance data. At run-time, OTM and EHCRS execution is performed concurrently with p-assertion recording.

TR-3-6: The system should be able to archive recorded provenance data.

Requirement applies to: OTM (marginally), EHCRS (marginally)
Accepted requirement: yes
If rejected, then reason: -
Deployed implementation feature: The provenance data recorded by OTM and EHCRS subsystem can be archived by the Provenance Stores.

TR-3-7: The system should be able to export recorded provenance data for external usage.

Requirement applies to: OTM, EHCRS
Accepted requirement: yes
If rejected, then reason: -
Deployed implementation feature: The provenance data recorded by OTM and EHCRS can be exported by means of export functions in the EXIST interface. To avoid a personal data protection risk similar to the one arising in AR-1-5, individual p-assertions have been anonimysed and include no medical information as part of its contents.

2.1.2.4 Utilisation of provenance data

TR-4-2: The architecture should support the dynamic processing of provenance data, i.e. recorded provenance data should be instantly queriable even if a recording session (recording of interrelated provenance records belonging to e.g. the same workflow) is still in progress.

Requirement applies to: OTM (marginally), EHCRS (marginally)
Accepted requirement: yes
If rejected, then reason: -
Deployed implementation feature: This functionality is supported by the provenance architecture. OTM does not make use of such functionality. The EHCRS subsystem continuously records p-assertions and dynamically retrieves recorded provenance data to collect complete patient record during while a recording session (recording of interrelated provenance records belonging to the same workflow) is still in progress.

2.1.2.5 Operation of the provenance architecture

TR-5-3: The provenance architecture should be deployable as an integrated part of a system, as a service within the same administrative domain as the client system and as a 3rd (external) party operated service, too.

Requirement applies to: OTM, EHCRS
Accepted requirement: yes
If rejected, then reason: -
Deployed implementation feature: In OTM's case, the internal architecture of the application includes a middle layer between OTM and the provenance API. This allows to deploy the provenance architecture as an integrated part of a system, as a service within the same administrative domain as the client system and as a 3rd (external) party operated service with minimum changes in the middle layer. The provenance architecture is deployed and an integrated part of the EHCRS subsystem in order to support the retrieval of complete patient records.

2.1.2.6 Interface

TR-6-2: Human-computer interfaces presented by the system for analysis and reasoning should be designed to allow multilingual support

Requirement applies to: OTM, EHCRS
Accepted requirement: yes
If rejected, then reason: -
Deployed implementation feature: OTM provides the human-computer interfaces for both OTM and EHCRS. The internal architecture has been designed to fully support multiple languages.

TR-6-5-A: Provenance information should be trackable on human-computer interfaces presented by the system at set level (e.g., database table, or spreadsheet).

Requirement applies to: OTM, EHCRS
Accepted requirement: yes
If rejected, then reason: -
Deployed implementation feature: OTM and EHCRS can use the Provenance Trace Portlet to display graphically traces built from the p-assertions they record.

TR-6-6-A: Provenance information displayed by the system on a HCI should be updatable on user request.

Requirement applies to: OTM, EHCRS
Accepted requirement: yes
If rejected, then reason: -
Deployed implementation feature: OTM includes in its human-computer interface a button to request the updated display of provenance information.

2.1.3 Constraint User Requirements

2.1.3.1 Performance constraints

Requirements on execution overhead due to provenance data generation and handling:

CR-1-1-A: Provenance recording should not impede a human entering data in real time.

Requirement applies to: OTM, EHCRS
Accepted requirement: yes
If rejected, then reason: -
Deployed implementation feature: The invocation time of the provenance service is negligible compared to a human entering data. The recording step is done asynchronously from the main execution flow in both OTM and EHCRS.

Requirements on storage overhead due to provenance data generation and handling:

CR-1-2-A: Recorded provenance data should not exceed 20% of overall system record data.

Requirement applies to: OTM, EHCRS
Accepted requirement: yes
If rejected, then reason: -
Deployed implementation feature: Recorded provenance data does not exceed 20% of overall system record data. The patient records are the biggest portion of record data, as it includes administrative and medical information about all patients, including imagery data. The policy of not including medical data inside the provenance store (for security and privacy reasons) has also contributed to fulfill this requirement.

2.1.3.2 Legal and ethical issues

Transplant application legal issues: The following four laws bound all activity in the area of organ/tissue transplantation:

1. Law 30/79, 28th October, 1979: On the extraction and transplantation of organ.
2. Orden Ministerio de Sanidad y Consumo 29th June 1987: testing for HIV in operations of procurement and implantation of human organs.
3. Real Decreto 411/1996, 1st March, 1996: Regulation of activities relative to the use of human tissues.
4. Real Decreto 2070/1999/30th December: regulating activities related to the procurement and clinical usage of human organs and tissues.

In addition to these activities are covered by more general medical laws – the most important of these are:

- The element of the Hippocratic Oath which states that a physician should preserve a patient's privacy
- Spanish national electronic data protection policies.

Requirement applies to: OTM, EHCRS
Accepted requirement: yes
If rejected, then reason: -
Deployed implementation feature: In health care applications such as OTM and EHCRS enforceable privacy rules are extremely important. Individuals share a lot of sensitive, personal information with their doctors like physical conditions, personal

habits, sexual practices, mental state, medications, family history, etc. Full disclosure is necessary for proper diagnosis and treatment. Patient information is then shared with many people, including doctors, hospitals, pharmacies, employers, relatives, schools, researchers, insurance companies, pharmaceutical companies, public health officials, and even the press and marketers. Many of these disclosures are necessary to treat patients, process claims, measure outcomes, and fight disease, therefore privacy protection should not be focused on nondisclosure, but on controlled and irreversible disclosure, which mainly means the protection of the identity of the patient. By introducing provenance recording in both OTM and EHCRS, new privacy issues had to be solved: while for provenance we need as much information as possible about the whole process (*who* did *what* and *when*) to be able to trace back all that has happened, for privacy we need to restrict as much as possible the information available in order to avoid identification of patients and practitioners by unauthorised users.

We analysed the risks of using distributed provenance stores to register all relevant information in OTM and EHCRS and identified a specially relevant risk: the *cross-link risk*. This is the risk that unauthorised users are able to link some piece of medical data with an identifiable person by cross-linking information from different sources. In both OTM and EHCRS we applied two policies to handle the cross-link risk: a) we do not put any medical or administrative data about patients in the provenance store that can be easily used to identify the patient, and b) even though medical information is not stored in the provenance store, we anonymise the patient data.

2.1.3.3 Security related issues

CR-4-2: The provenance architecture should allow both automated and manual determination of access control rights on recorded provenance data.

Requirement applies to: OTM (indirectly), EHCRS (indirectly)
Accepted requirement: yes
If rejected, then reason: -
Deployed implementation feature: Both OTM and EHCRS make use of the access control mechanisms provided by the provenance architecture. On top of that, both OTM and EHCRS have its own user access control mechanism, based on user authentication.

2.1.4 User Requirements that do not apply to OTM and EHCRS

Some of the user requirements from the organ transplant scenario that were included in [D2.1.1] were not addressed to the applications but to the underlaying provenance architecture. For completeness in this section we provide the list of user requirements which do not involve direct contribution from OTM and EHCRS.

TR-6-1: The architecture should support a rich set of generic APIs that allow analysis and reasoning tools to be built upon.

TR-6-6-B: HCIs presented by the provenance system for provenance monitoring should support continuous monitoring, i.e. the displayed information should be updated automatically on every change as soon as possible.

CR-4-1: The provenance architecture should have a configurable, fine-grained access control system over recorded provenance data.

CR-5-1: The provenance architecture should have good application fit, meaning: meet the basic logging needs and have additional potential for more complex questions outlined in the scenario description.

CR-5-2: The provenance architecture should have the properties of cost efficiency and robustness versus an in-application hand-engineered logging system.

A summary of all the user requirements relevant for the organ transplant scenario is available in Appendix A.1.

An Evaluation of these requirements can be found in other documents:

- An analysis on all these requirements can be found in [D2.2.1], where each of these has been translated to one or more software requirements. A sumamry of this connection between user and software requirements is available in Appendix A.2.
- The way the Provenance architecture addresses the software requirements can be found in Deliverable D3.1.1, "An Architecture for Provenance Systems" [D3.1.1], Chapter 9.
- The way the Provenance tools address the software requirements can be found in Deliverable D6.1.1 "Tools Description Document" [D6.1.1], Chapter 2.
- Provenance Server fulfillment of user and software requirements can be found in Deliverable D9.3.3a "Client Side Library Design and Implementation" [D9.3.3a], Chapter 2.

2.2 Fulfillment of the technical requirements

In this section we evaluate the fulfillment of the technical requirements in [D2.2.1] that were related with the organ transplant management scenario. In order to identify which are these software requirements, a summary listing all the software technical requirements relevant for the organ transplant scenario is available in Appendix A2.

It is important to note that the software requirements from [D2.2.1] were not focused in the application functional requirements, but in the software requirements the underlaying provenance architecture should fulfill to support these applications. Therefore, in the following subsections only the contribution of the OTM and EHCRS applications to the fulfillment of these requirements will be evaluated. For completeness, the rest of software requirements which do not involve direct contribution from OTM and EHCRS are listed in section 2.2.4.

2.2.1 Functional requirements

2.2.1.1 Basic Functional requirements

SR-1-2: The provenance architecture should allow the retrieval of a provenance trace from the Provenance Store. Either a complete trace or a subset may be retrieved.

Requirement applies to: OTM (indirectly), EHCRS (indirectly)
Deployed implementation feature: Both OTM and EHCRS record the p-assertions related to the different steps of the transplant management, retrieval of patient records used in the arguments, contributing factors and intermediate results which lead to a particular decision. A provenance trace is then retrieved by OTM and EHCRS directly through the API, or by the tools graphical interface.

SR-1-5: The provenance architecture should allow the results of a query to the Provenance Store to be captured for future use. A query in this context must be specified with reference to the structure of the Provenance Store.

Requirement applies to: OTM, EHCRS
Deployed implementation feature: Both OTM and EHCRS can capture the results of as provenance query and use them for future use, including the creation of a new query depending on the results of the previous one.

SR-1-7: The provenance architecture should allow a user to verify the contents of a Provenance Store against a specified set of rules. Verification in this context means that the contents of the Provenance Store meets the set of constraints expressed by the set of rules.

Requirement applies to: OTM
Deployed implementation feature: Rules have been expressed following JESS format. These rules can be imported into the Rule Analysis tool. OTM can then use the Rule Analysis tool to check if the recorded decisions and steps in the process follow the rules. Internally OTM also makes some automatic enforcement of the rules, although allows some flexibility in some cases (e.g. to allow requesting a test without all the pre-conditions holding, for emergency purposes).

SR-1-8: The provenance architecture should allow a user to specify a time period in the future at which a provenance query may be submitted to a Provenance Store. A scheduler will be made available that allows queries to be stored to disk, and dispatched to the store in the future.

Requirement applies to: OTM, EHCRS
Deployed implementation feature: As p-assertion recording is done asynchronously, This feature is not used in the deployed implementation.

2.2.1.2 Additional functional requirements on the provenance system

SR-1-12: The system should support the recording of different provenance information views related to an event or an entity.

Requirement applies to: OTM, EHCRS
Deployed implementation feature: Both OTM and EHCRS record their own view of interactions, vby using the views defined in interaction p-assertions.

SR-1-17: The provenance architecture should be deployable as an integrated part of a system, as a service within the same administrative domain as the client system and as a 3rd (external) party operated service, too.

Requirement applies to: OTM, EHCRS
Deployed implementation feature: in OTM's case, the internal architecture of the application includes a middle layer between OTM and the provenance API. This allows to deploy the provenance architecture as an integrated part of a system, as a service within the same administrative domain as the client system and as a 3rd (external) party operated service with minimum changes in the middle layer. The provenance architecture is deployed and an integrated part of the EHCRS subsystem in order to support the retrieval of complete patient records.

2.2.2 Performance requirements

SR-2-1: The additional execution overhead for an application recording provenance information should be kept to a minimum.

Requirement applies to: OTM, EHCRS
Deployed implementation feature: The internal architecture of OTM and EHCRS makes a separation between the execution of the system and the asynchronous recording of provenance data. At run-time, OTM and EHCRS execution is performed concurrently with p-assertion recording.

SR-2-2: Storage space requirements of the provenance architecture for provenance information recording should be kept at a reasonably low level.

Requirement applies to: OTM, EHCRS
Deployed implementation feature: The Provenance Store requires reasonably low amount of storage space. The policy of not including medical data inside the provenance store (for security and privacy reasons) has also contributed to fulfill this requirement.

2.2.3 Operational requirements

SR-4-1: Provenance information displayed by the provenance architecture on a HCI should be updatable on user request.

Requirement applies to: OTM, EHCRS
Deployed implementation feature: The provenance information displayed on the tools graphical interface is updateable on user request.

SR-4-4: Human-computer interfaces presented by the provenance tools should be designed to allow multilingual support.

Requirement applies to: OTM, EHCRS
Deployed implementation feature: OTM includes in its human-computer interface a button to request the updated display of provenance information.

2.2.4 Other functional requirements that do not apply to OTM and EHCRS

A summary of the software technical requirements relevant for the organ transplant scenario is available in Appendix A2.

As mentioned in the introduction to section 2.2, some of the software requirements in [D2.2.1] which come from organ transplant scenario user requirements were not addressed to the applications but to the underlaying provenance architecture. For completeness in this section we provide the list of technical requirements which do not involve direct contribution from OTM and EHCRS.

SR-1-1: The provenance architecture should provide for the recording and querying of interaction and actor provenance.

SR-1-3: The provenance architecture should allow the back-up of a Provenance Store to be taken. This will generally include an archiving facility that allows data within a Provenance Store to be saved for future use.

SR-1-4: The provenance architecture should allow comparisons to be made across Provenance Records within a Provenance Store with reference to particular data attributes within a Provenance Record.

SR-1-9: The provenance architecture should allow capabilities provided by the tools to be accessible as an API. This is to allow such capabilities to be embedded within an existing application.

SR-1-13: The provenance architecture should support the migration of provenance data among provenance stores.

SR-3-1-1: All of the functions of the provenance architecture should be accessible through its API so it can be used as an embedded component in a system.

SR-3-1-2: The provenance architecture should support a rich set of published, generic APIs that allow application specific analysis and reasoning tools to be built upon.

SR-3-2-1: Export formats for provenance data should be non-proprietary to allow tools and applications to be built without violating IPR rules. A format based on an existing data representation standard (with special focus on XML defined by XML Schema) would be highly preferred.

SR-4-2: HCIs presented by the provenance architecture for displaying the contents of a Provenance Store should support continuous monitoring, i.e. the displayed information should be updated automatically on every change as soon as possible.

SR-6-1: The provenance architecture should have a configurable access control system over the resources it provides, with a granularity that is sufficient to protect these resources.

SR-6-2: The provenance architecture should allow both automated and manual determination of access control rights.

SR-7-1: The provenance architecture should have the properties of cost efficiency and robustness versus an in-application hand-engineered logging system.

Evaluation of these requirements can be found in other documents:

- The way the Provenance architecture addresses the software requirements can be found in Deliverable D3.1.1, “An Architecture for Provenance Systems” [D3.1.1], Chapter 9.
- The way the Provenance tools address the software requirements can be found in Deliverable D6.1.1 “Tools Description Document” [D6.1.1], Chapter 2.
- Provenance Server fulfillment of user and software requirements can be found in Deliverable D9.3.3a “Client Side Library Design and Implementation” [D9.3.3a], Chapter 2.

2.3 Summary

In this chapter we have provided a technical evaluation of the OTM and EHCRS applications based in the analysis of the fulfillment of the requirements identified in [D2.1.1] and [D2.1.1]. We have evaluated, for each requirement, which application (OTM, EHCRS) it applied to, and the way the applications contribute to the fulfillments of the requirement.

As software requirements in [D2.2.1] were abstracted from the applications and are more focused in requirements for the underlaying provenance architecture, the client-side libraries, and the tools, an evaluation of the OTM and EHCRS applications solely based on requirements fulfillment analysis would be incomplete. Next chapter provides an evaluation on both applications by means of the execution of some test scenarios.

3 Functional evaluation

In the previous chapter we have evaluated the OTM and EHCRS applications by analysing how they comply with the user and software requirements from Work Package 2.

In this chapter we will evaluate the system by running some test scenarios, and analysing how useful are the results provided by the system. With these scenarios we aim to show that the use of provenance bring 3 main benefits:

Benefit 1: The provenance-aware OTM system can produce at run-time an explicit representation of the distributed medical process actually taking place. This process can then be graphically viewed through the visualization tool

Currently the task to get a trustworthy summary of the whole distributed transplantation process from scattered reports (most of them in paper) located at different institutions would be a very time-consuming task. This is not only due to the lack of use of IT solutions in organ transplant management in Spain: even if there were several medical applications logging all the events in their local logging systems, it would be a time-consuming task to integrate all the information scattered in the different logs to create a single, unified representation of a distributed case.

Benefit 2: The provenance-aware OTM can query and analyse the aforementioned representation in order to extract valuable information to validate, e.g., the decisions taken in a given case, or to make an audit of the system over a period of time.

Not only an explicit representation of the medical process is created, but this representation is structured in a way that eases querying an analysis. It is clear that these activities would be very time-consuming in current organ transplant management, even if the collection of the different reports had been done already.

Benefit 3: As a side effect, provenance documentation can be used to have a unified view of a patient's medical record with its provenance

That is, provenance documentation provides a way to connect each part of the medical record with the processes in the real world that originated it and/or the individuals, teams or units responsible for each piece of data.

This chapter is structured as follows: in section 3.1 we present the scenario setup. Then in section 3.2 we describe the three test scenarios that we use to evaluate the system. In section 3.3 we make some evaluation about the results. Finally in sections 3.4 and 3.5 we present the evaluation provided by users.

3.1 The Test scenario setup

In order to test the system, we have created a demonstration setup which includes some hospitals, testing laboratories and a coordinating Organ Transplant Authority. Figure 2 summarizes the different administrative domains (solid boxes) and units (dashed boxes) that are involved in the test scenarios.

The actors in the system are:

- *1 Retrieval Hospital (Hospital A)*: hospital offering a donation and coordinating / carrying out the retrieval of the organ(s).
- *2 potential Implantation centers (Hospital B and Hospital C)*: hospitals receiving the organ offers evaluate them and, if an organ is allocated to them, carrying out the implantation of an organ to a recipient in their waiting lists..
- *3 Test Laboratories within hospitals (Lab A, Lab B, Lab C)*: specialist medical units within the hospitals performing standard tests (blood, urine) to determine the health condition of a patient.
- *1 Specialized Test Laboratory (Lab D)*: a separate center for performing specialized tests (HLA analysis or crossmatching for example).
- *1 Regional Organ Transplant Authority (OTA)*: regulatory and oversight body for all transplants in a given region. Associated with a number of retrieval / implantation centers. The OTA center also acts as the coordinating point to find recipients if local recipients are not available. The OCATT is the Catalan OTA which coordinates the area of Catalonia, Valencia and the Balearic Islands. For the rest of Spain, ONT acts as OTA.

The figure also shows the 5 provenance stores (PSa, PSb, PSc, PSd, PSo) that will be located in different security domains and which will be linked in order to provide integrated results.

The demonstration will consist of several transplantation management scenarios. For each scenario, one or more hospital units may be involved: the hospital transplant unit, one or several units that provide laboratory tests and the unit that is responsible for the patient records (which will use the EHCRS application services). The test scenarios are described in the following section.

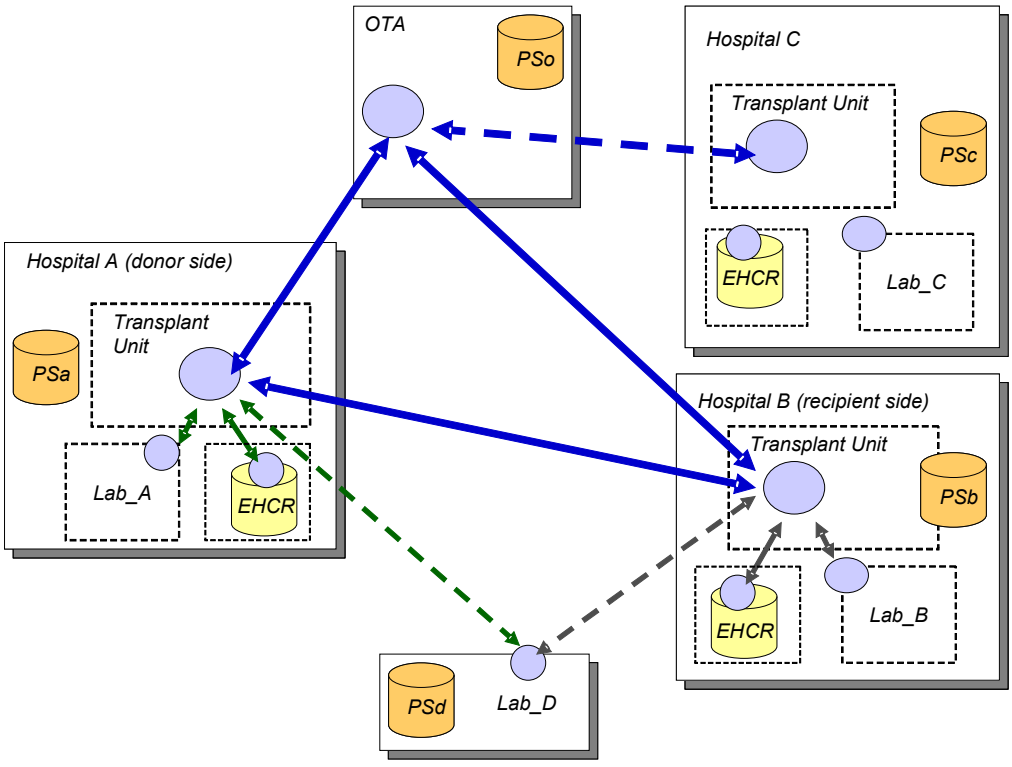


Figure 2 -- Actors involved in the demo.

For more details please see Appendix B

3.2 The three test scenarios

3.2.1 Scenario S1

In this scenario we show how a medical history and EHCR is started, updated and queried. This scenario aims to show the functionalities of the EHCR system without the mediation of the OTM system.

The scenario run has two steps:

S1.1 A patient called Mr. Anderson is registered in OCATT with his national insurance number. This event starts Mr. Anderson medical history in the system.

S1.2 Mr. Anderson's EHCR is created in Hospital de la Vall d'Hebron and then updated in Hospital Clinic.

After the run, two queries are perfomed:

- Mr. Anderson's EHCR is queried in Hospital de Sant Pau. The EHCRS in Hospital de Sant Pau finds no data about Mr. Anderson, but then some data is found in the EHCRS from Hospital de la Vall d'Hebron and the one from Hospital Clinic.
- Mr. Anderson's medical history is queried using the Tool of provenance.

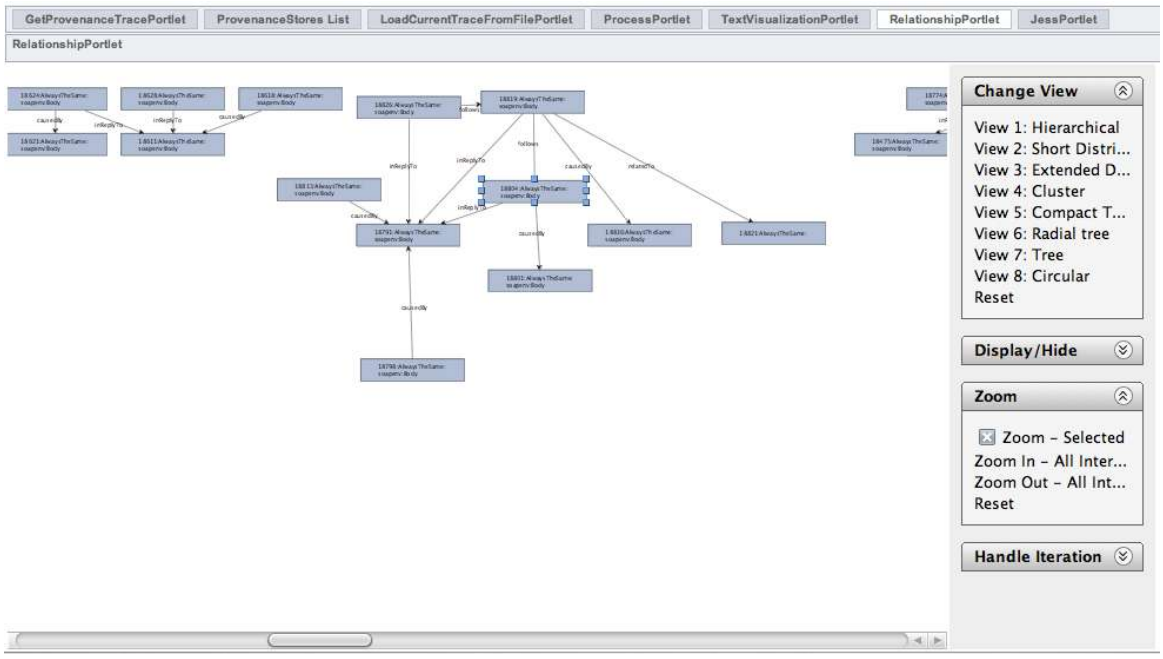


Figure 3 -- Querying Mr. Anderson medical process using provenance.

This first scenario shows how simple medical events are recorded in the provenance store and how this events create a medical process – the medical history or a case – of a patient. The results of query Q1.1 show how the recorded provenance information can be used to pull together the whole EHCR of a patient. Then Q1.2 shows how somebody can analyze a case or a whole medical history from the provenance information stored by the EHCRS.

The detailed, step-by-step description of the scenario is provided in appendix B.1.

3.2.2 Scenario S2

This scenario represents a transplant management case when everything goes smoothly (an almost "ideal" case). It shows how events are recorded by different actors in the scenario, and some examples of the queries that can be done.

The Scenario run consists of 18 steps. Patient Laura Gomez Ruiz appears in Hospital de la Vall d'Hebron. The EHCR for that patient was already in the hospital. The patient is declared as potential donor.; after getting the results from the tests a donation decision states that the heart and the liver will be donated; the offer is sent to the OTA, which forwards it to the first hospital candidate (Hospital de Sant Pau) which accepts both offers. An extraction team from Hospital de Sant Pau travels to Hospital de la Vall d'Hebron and, after extraction and close examination of patient A1 organs, decides that the liver is in no good condition to be implanted, but the heart is indeed in good condition. Extraction team returns to Hospital de Sant Pau and then implants the organ to patient Ramon Perez Perez .

After the run, 3 queries are performed:

- All the events related to a specific patient: The results of this query show the different events related to patient Laura Gomez Ruiz, including a) the events related to her entrance to the hospital, her status as potential donor, the tests requested and the organ decision made; b) the events related to the organ extraction phase. Figure 4 shows only part of the retrieved diagram, depicting the different tests carried out which were relevant for the liver offer (shown on the left).

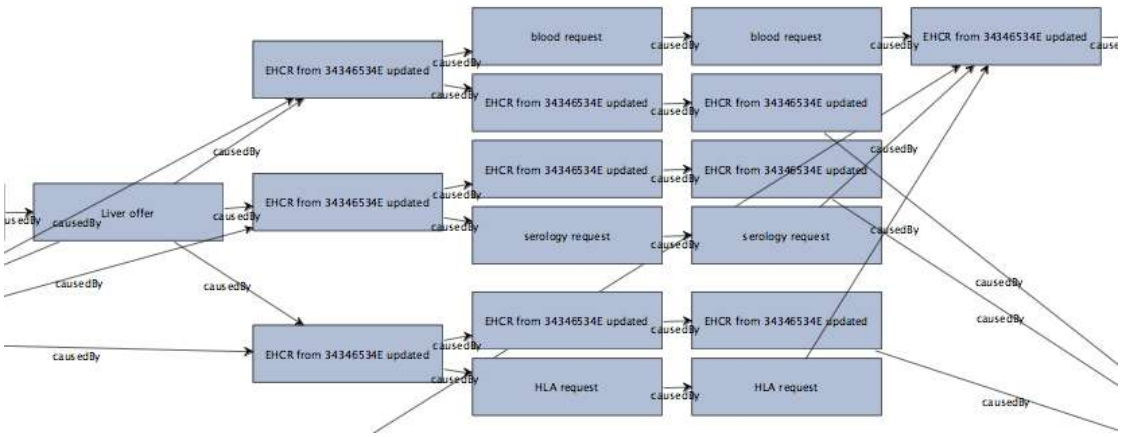


Figure 4 -- Querying Ms. Gomez Ruiz medical process events using provenance: tests related to the liver offer decision.

- Which users have recorded something for an specific patient: This is an example of a query that does not provide a provenance trace, but a textual output. The query result shows that three users have been involved in the recording of patient Laura Gomez Ruiz.
- All the events related to a specific heart donation case: The results show the different events related to the donation of the heart from patient Laura Gomez Ruiz, including a) the events related to her entrance to the hospital, her status as potential donor, the tests requested and the organ decision made; b) the events related to the recipient for the organ, including the tests requested and the recipient assignment c) the extraction and implant steps, d) the several logging of different actors into the system.

The detailed, step-by-step description of the scenario and all the query results are provided in appendix B.3.

3.2.3 Scenario S3

This scenario shows how provenance information of a previous transplant case is linked to the current case, and how it appears when querying for the full provenance of the current case.

The Scenario run consists of 7 steps. Patient Ramon Perez Perez from scenario S2 dies days after the liver implantation from causes that have nothing to do with the liver implantation; therefore, the team decides to declare patient Ramon Perez Perez as potential donor and offer the liver again for transplantation. No extra tests should be done and the liver offer is sent to OTA, which forwards it to the first hospital candidate (Hospital Vall d'Hebron) which rejects the offer again(because of the lack of reliable Biochemistry data). OTA forwards the offer to second hospital candidate (Hospital A) which accepts the offer. An extraction team from Hospital de Sant Pau travels to Hospital Clinic and, after extraction and close examination of Mr. Perez's organs, decides that the liver is in good condition to be implanted. Extraction team returns to Hospital de Sant Pau and then implants the organ to patient Carlos Garcia Quinones. Implantation fails (the liver is not performing well enough). The Hospital coordinator wants to know the provenance for this failure (solution: the Biochemistry data was not up-to-date, and the Biochemistry test from Lab A -which arrived too late and was not used in the decision) showed high levels of 2 substances that, if someone had noticed, could point out that the liver was already in no good condition).

After the run, 2 queries are performed:

- All the events related to a specific patient: The results of this query show the different events related to patient Ramon Perez Perez as a donor in a similar way to scenario 2's donor. The difference is that this time the medical history of Mr. Perez includes the p-assertions from the previous scenario, where he was the recipient.
- All the events related to a specific liver donation case: The results show the different events related to the donation of the liver from patient Ramon Perez Perez including a) the events related to the donation phase including the donation decisions; b) the events related to the recipient for the organ, c) the extraction and implant steps, d) the several logging of different actors into the system (not shown in figure), and e) relevant events from the scenario 2 related to what happens in scenario 3).

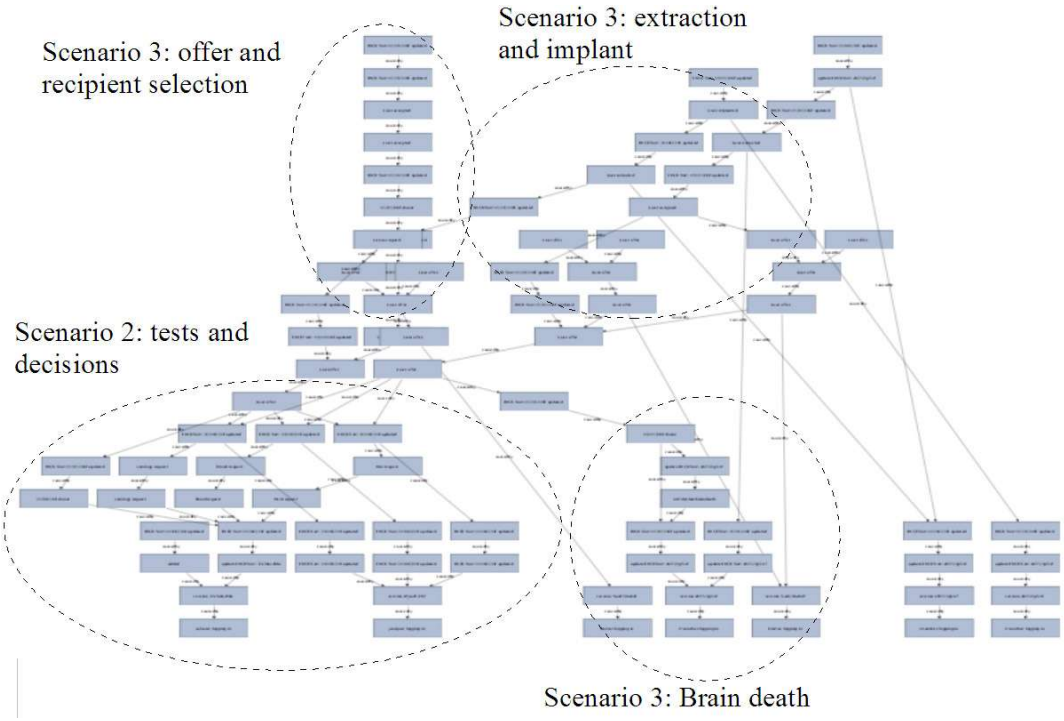


Figure 5 -- Querying the events related to a liver donation case using provenance.

This scenario shows how past p-assertions related to the past medical history of the patient can be connected to a current scenario.

The detailed, step-by-step description of the scenario and all the query results are provided in appendix B.3.

3.3 Our evaluation

In this section we will evaluate the results shown in the three scenarios by connecting them with the three benefits for provenance-aware OTM and EHCRS.

Benefit 1: The provenance-aware OTM system can produce at run-time an explicit representation of the distributed medical process actually taking place. This process can then be graphically viewed through the visualization tool

Benefit 1 is clearly shown in the three scenarios, and more specifically in queries Q1.2 (see section B.1), Q2.1 (see section B.2) and Q3.1 (see section B.3).

Benefit 2: The provenance-aware OTM can query and analyse the aforementioned representation in order to extract valuable information to validate, e.g., the decisions taken in a given case, or to make an audit of the system over a period of time.

Benefit 2 is clearly shown in scenario 2 and 3, where we can extract not only the full representation of all events, but specific information (including textual information resulting from analysis of the p-assertion contents, as in Q2.2 (see section B.2).

Benefit 3: As a side effect, provenance documentation can be used to have a unified view of a patient's medical record with its provenance

Benefit 3 is shown in all scenarios, as the provenance documentation extracted connects parts of medical record with the individuals, teams or units responsible for each piece of data. Scenario 3 also shows how the provenance documentation can be used to unify the different recordings of the medical process carried out to a patient in a single view, something that would be difficult to achieve with a standard logging system.

3.4 User evaluation

To complete the evaluation of both OTM and EHCRS, we showed the same three scenarios to some potential users of the system.

The first difficulty we had to address was to get a good set of users. Several hospital transplant coordinators and administrative members of the OCATT were invited to attend the demonstration. However it was really hard to synchronize agendas as, because of the 24-hour emergency nature of organ transplant management, almost all of the people invited should be available at any time to attend a transplant case.

As an alternative, we received the invitation from Hospital de Sant Pau transplant coordination team to make our demonstration as part of an exercise to their students in a master course on transplant management the team in Hospital de Sant Pau is involved in. It is important to note that some students are already members of units involved in transplant management; they attend the master course to receive a qualification. This provided us with a variety of potential users similar to the ones we were aiming at:

- people with a medical profile: students with a medical background, which are already or will become members of a transplant unit staff.
- people with an administrative profile: students with an administrative or management background, which are already or will become members of the administrative staff in the OTA or a hospital.

The second difficulty we had to address is the effects of a moderate *digital divide*: quite a lot of the students are not skilled computer users. The computer skills of our user group ranged from users that avoid computer usage to normal users with some basic computer skills to users that are proficient in the use of standard software tools and/or office suites. Therefore, these users would hardly be able to evaluate in detail all the functionalities of the system and, in special, the full extent of the functionalities provided by the provenance extension of the system. So we had to design the questions and the evaluation session in terms they could fully comprehend, such as the impact of a given functionality to the medical practice. We also added some questions to make the users evaluate to some extent the three benefits mentioned at the beginning of this chapter.

Next section describes the organization of the user evaluation sessions, and then in 3.4.2 a summary of the questions and answers is provided.

3.4.1 Organization of the user evaluation sessions

The session was organized with an informal atmosphere, based on continuous interaction from the users, to try to reduce the negative feelings some users have using computers. The session started with a short presentation about the OTM-EHCRS system where we gave a high-level description of the components in the system, including the provenance stores.[1]

1 There is no direct translation of the provenance concept neither in Spanish nor in Catalan. The closest terms would be "origen" (*origin*) or "linaje" (*lineage*). This posed an extra difficulty when trying to explain the

Then we made an interactive demonstration of the system, picking some users to play the roles of some of the actors in the scenarios: a surgeon in hospital A, an OTA manager or a laboratory assistant. Questions about the OTM functionalities, EHCRS functionalities and on how to do particular steps of the process were raised during the demonstration. These questions are not reported in this section as they were not related to the provenance aspects of the system.

The demonstration ended with the usage of the tools to analyze the provenance documentation generated in the simulated scenarios: this part was the one that triggered the most questions, as they are not used to see this kind of information. Some time was spent on close inspection of the diagrams to see the causal relations in the three scenarios, and specially on the provenance for the medical decisions.

The final part of the session was an interactive debate to extract their opinions to the system. We discarded the idea of them having to fill in forms because then it is hard to control if their answers are informative (we should take into account that none of them is a computer scientists). By the use of interactive dialogs we could:

- ask extra questions or clarifications if an answer was not clear or informative enough;
- focus the user attention on the provenance aspects of the system, (the system was something new for them so they tended to make comments and ask questions about the non-provenace functionalities of the OTM-EHCRS system).

3.4.2 User evaluation results

The following is an extract and translation from the final part of the user evaluation session: the question and answer dialog. Here we have deleted the parts that were not related to the provenance aspects of OTM-EHCRS.

Part 1: PROVENANCE HANDLING

Q: *Could you summarize how is everything recorded right now?*

Some students (with some guidance from the lecturers) gave a summary of the different ways medical processes are recorded right now. The list included a) written notes, b) faxes between centers, c) phone calls and d) extensive documentation, which in most hospitals is filled in paper forms, stored in standard files and archives, with some exceptions for special tests in some hospitals.

Q: *So all the documentation in paper format is stored in some file archive, but is there any register of phone calls?*

The phone operator tries to keep a record (a paper form) with the calls made, but it it usually filled after these calls are made, to not interrupt the main activities carried out during the call.

Q: *How are all these reports and files processed for future usage?*

They are archived in different parts. Medical notes about a patient go to the patient medical record. Notes about the transplant management go to special case files. Faxes and phone calls have their own file. This may change from hospital to hospital.

concept to the users.

Q: *Which are the main differences you see with the way things are recorded and processed in OTM-EHCRS? Are they positive or negative?*

A discussion was triggered with this question. The users, although used to doing things in the current manner, agree that without such a system obtaining information dispersed across different units or organisations is problematic. However, any new system will require a period of adaption.

One of the lecturers leaded the discussion back to the question: currently it is very hard to get additional information from other units or centers, and the OTM-EHCRS system eases this.

Part 2: IMPACT ON THE NORMAL MEDICAL PRACTICE

Q: *Do you see any important impact on the medical practice by using the system?*

Another discussion was triggered again around the idea of users having to get used to the system.

Then most of the users agreed that, apart from having to use a computer instead of paperwork, it mostly requires the user to introduce the same information than now.

Some students mentioned that the system may create new habits in the user. Currently staff uses to bring the paper forms to be filled with them while they perform their activities on each step in the process. This allows them to fill in some of the information in the final form during the medical process. Later the forms are checked and filed in the archive. But then with OTM the user would have to either carry a laptop or a PDA with him to fill the forms during his medical practice, or take some notes and then go to a computer to introduce the case in the system. Then one of the lecturers mentioned that this is already the procedure followed for some things that are already stored in computers in other hospital units, even though most of things are registered still in paper. Another lecturer said that the change (to computers) is coming anyway, so sooner or later staff will have to adapt to computers.

Q: *Does it introduce any temporal delay?*

The students that took part in the demonstration mentioned that it takes a bit longer than to fill in a paper (one of them considered that it may be because the students testing the system were not used to it). But two students saw some positive effects, as the system can save time in some administrative issues such as calling the OTA, faxing documents, waiting for lab results to come back physically by courier, etc.

One of the users also mentioned that it is good that the user is not obliged to stop what he or she is doing to record anything happening, but the system allows the user to report it later. One lecturer added that this kind of flexibility is good in a transplant unit, where there are some steps in the process that are time-critical.

Q: *But delaying the introduction of information into the system may introduce some imprecision in the reporting. Is this risk well-balance?*

This question was answered mainly by lecturers. In transplant units there are some moments that all staff members are too busy to stop what they are doing to fill in a form, be it on paper or be it through a computer. It would be stupid to stop a surgery to properly document what is happening, or to have a person in the team unable to do anything else than sitting down in front of a computer and entering data into the system.

As a summary, delayed reporting is something that may introduce some error, but there is no other solution in the time-critical steps of transplant management. And the system does well in providing such flexibility.

Part 3: PROVENANCE USES

Q: *The most obvious usage of the provenance recording is for legal audit, that is, for post-event incident investigation. Could you summarize how is this currently done?*

Some students (with some guidance from the lecturers) tried to give a summary of the process. The most valuable input was from a lecturer, which described it as a painstaking process involving a) the search for all the archived documents related to a case, b) interviews with the transplant to coordinator and the staff members of the unit, c) visits to other institutions that were involved in some steps of the process. Sometimes information is missing and should be completed with extra inquires (e.g., the date and time of the phone calls made during an incident, if they were not properly recorded).

Q: *Which are the main differences you see with the introduction of the OTM-EHCRS system?*

The same lecturer answered that the main difference he could see is that the system already gives the auditor a summary of each donation case, all the units involved and the sources for any decision. It gives already a kind of overview, plus it provides the auditor or the investigators with pointers on where to look.

Q: *Is it enough the information displayed in the tool? Is it useful?*

One of the users that was involved in the demo said that the graphical representation shows the connections between the different events and steps in the process, so this was very useful in his view. Another lecturer mentioned that sometimes it may take some time to analyze the diagram, that is a bit complex.

Q: *Do you think this complexity is because of the way the tool represents things? Or is it typical of this kind of processes?*

The lecturer guessed that it may well be because of the transplant management process. Incidents are distributed processes that are split in different locations but they have quite a lot of inter-connections. The graphs created by the tool require some effort to be understood, but it is far less than the time it would require a human auditor to find out all these connections by himself.

Q: *Then, do you find the results provided by the system useful?*

The lecturer was positive about this. It will shorten a lot the time needed to collect information and re-construct what happened.

Q: *Does it record all the important steps in the process?*

The same lecturer answered that actually it seems to record quite a lot of steps. Some of them seem a bit too low-level, such a the login steps of users, but he was unsure if that was good or bad. One of the students said that this information may be important to certify which user did what in the system.

Q: *Another usage for this kind of process recording is for internal auditing, that is, to provide the medical units with a tool to internally check how the process is going or to analyze past cases. Is it useful for internal usage?*

One of the senior lecturers said that it could be useful indeed. He warned that it may not be really useful to be used during the transplant case management, as staff does not have too much time to sit down in front of a computer, but he could see the interest of some post-incident analysis. He found interesting to see the results of the queries, specially the graphs showing all the connections, and where did the information come from at any step in the process. The same for the decisions, to see the sources of data, who was involved indirectly in a decision. He actually found it a bit shocking, as this is something (transplant) coordinators usually do not have: they only consider who was involved in a decision and where the information for that decision came from, but do not think who created that information, maybe because now it is something hard to find out.

Q: *Is the information displayed enough?*

The lecturer answered that it was more than enough, actually he got the impression that it gave too much detail in the process. But then he wondered if it was just a matter of getting used to the representation.

Q: *What about decision points? Is there enough information?*

This question created a small debate. Two of the students involved in the demo said that it was one of the most surprising things to see: not only the direct inputs of a decision but also all the steps in the chain that generated such input. This is something that users do not have now.

One student mentioned that, from her perspective, it looked a bit too restrictive the fact that the system could not identify which part of a given test a decision was based on, only the whole test. That is, the system could only identify that a given decision was based on test A or on report B, but not on which part of the test or the report is based. For that the human has to have a look into the report or the test.

Q: *But then the user would have to provide more detail when entering the decision into the system. Going into each of the tests and/or the reports and selecting the fields that are most relevant to the information. Wouldn't that be too time consuming?*

This question triggered a live debate. Two lectures and one of the students involved in the demo considered that this would mean to spend too much time to record any single decision, and that an auditor would tend not to fully trust this information, going back to the full test or report to check for himself if there was something missing. After some arguments and counterarguments, an agreement was reached that the system seemed to provide a good equilibrium in this aspect. It asks for enough information to provide a link, but not asking too much from the user.

Q: *The system is able to detect unacceptable delays in the process, and missing steps in the process. What do you think about this functionality?*

Some students found strange that the system allows to miss steps in the standard transplant management process and considered that the system should forbid to miss one step, if that was mandatory by the regulations. But then one of the lecturers reminded the flexibility issue, and why sometimes it s is good to be able to start next step (e.g. order a test) without having completed the previous ones. Medicine is plenty of exceptions to the rule. It is good that the system is flexible enough to allow the medical team to alter the process, and it is good that this deviation is recorder to be checked later on.

Then discussion moved back to the question. One of the lecturers considered that it can be useful to have some quick performance analysis, to detect bottlenecks and to detect missing steps. Currently it is hard to assess time delays, as time is recorded differently for different steps in the system. Missing steps are hard to detect unless they are obvious.

Part 4: OTHER USAGES

Q: *Can you see, or foresee, other potential usages for the process information recorded by the system?*

One student said that, apart of its uses to improve team unit performance (analyzing small deviations and such), the tool may be used to try improving the medical policies themselves, that is, to detect problems arising one time and one time again (e.g., bottlenecks) which are produced by the medical policies defined by the OTAs.

Another student said that the results of the analysis may be used in some way to be the base for scientific reports or publications, documented by the cases the user can query with the tools.

Part 5: QUESTIONS FROM THE USERS

Most questions were clarifications on things previously discussed, or questions unrelated to provenance aspects. The following were the only two questions related to provenance aspects.

Q: *Can users add new queries apart of the fixed ones?*

Our answer was negative, as it is not easy to create the queries. System administrators can create queries and add them to the list of queries a user can select, if needed.

Q: *Why only information about transplant procedure is shown? Why not other medical processes in other medical units?*

Our answer was that what we showed was a demo which only recorded the medical steps directly related to organ transplant management. To record all the information to properly document a medical process the computer applications in all medical units should be adapted. The idea is that, in the future, all the systems in a hospital should be adapted in order to provide this information.

Part 6: WRAP UP. FINAL QUESTION

Q: *Said all that, if you compare the difficulties of adapting to a new way of doing things with the extra functionalities it provides, what would be your opinion?*

There were some laughs when two students, which are currently performing administrative tasks, quickly answered that they would love to have it running, as it would make their life easier. Specially for those like them that currenly are obliged to make phone calls and send faxes.

A discussion started again about having to adapt to the system, and about changing the way things are done right now. As a summary, some other users consider that it would take some time to adapt, but in the end they would accept it.

3.5 Summary of user evaluation

In general the evaluation has been positive. We already expected that it would be not convenient to use their answers to do a complete evaluation about OTM-EHCRS provenance functionalities system, as it is hard for these users to fully understand the full implications of the provenance concept.

It took some effort to keep the discussion alive and focused. A concern that was raised more than once is about having to change the way they currently work. This is not uncommon to these kind of users, and we were already expecting some aversion to change. But it is important to remark that some attendees recognized that some adaptation to computers will happen anyway sooner or later. Another interesting fact to remark is that, despite the fact that they tended to discuss about the (medical) incident management aspects of the application, some answers also showed that some of them started to realize some potential positive impact of the provenance part of the application, even though they could not fully understand the concept.

After the end of the session, some informal discussion started about the recording of all this information being some sort of "big brother". Some of the attendees expressed the concern of this system becoming a weapon against the medical practitioners, to question any single action or decision. Some senior attendees said that actually, if properly used, it could work in the opposite direction: it could improve confidence in the organ transplant management units, to tell the patient everything is controlled and checked. And it can be useful to the staff members themselves, to make internal analysis (not legal auditing) about their actions and learn from their mistakes.

Appendix A Summary of User and Software Requirements

A.1 Mapping of User Requirements to Software Requirements

A.1.1 Abstract level capability requirements

URD ID, flags, source	*Text of User Requirement*	*SRD identifier*
AR-1-1 *essential*	The provenance system should support the following operation: Check a given set of decisions in a case against the established rules to ensure that it is conformant. These rules may or may not be automatically enforced by the transplant management software – however in the general case many of them will not be. This provenance question is a post-hoc check as to whether rules were followed. (asked by Transplant Authority, Families, 3rd parties)	SR-1-1, SR-1-2, SR-1-4, SR-1-7
AR-1-2 *essential*	The provenance system should support the following operation: Derive a trace of the arguments, contributing factors and intermediate results which lead to a particular decision. (asked by Transplant Authority, Families, 3rd parties, Physicians)	SR-1-1, SR-1-2
AR-1-3 *essential*	The provenance system should support the following operation: Derive aggregate information across many cases such as the percentage of incidents of a certain type, success rates by center, etc. (asked by Transplant Authority, researchers, physicians)	SR-1-1, SR-1-2
AR-1-4 *nice to have*	As an advanced feature the provenance system could support the following operation: Truth maintenance for "next best candidate" or other dynamic information. Advanced functionality: meaning that the system could be used to keep up to date precalculated lists of recipients ready for an incident. This is a type of result which may need to be modified as underlying data changes. (asked by transplant system itself, physicians)	*No SR: This application specific function should be implemented by application layer software components*
AR-1-5 *essential*	The provenance system should support the following operation: Extraction of an entire case-trace: gather all the records related to one incident into a single case-file. (asked by physicians, families, patients)	SR-1-1, SR-1-2
AR-1-6 *essential*	The provenance system should support the following operation: Identify all individual users related to an incident. (asked by physicians, Organ Transplant Authority, 3rd parties (legal challenges))	SR-1-1, SR-1-2, SR-1-4

URD ID, flags, source	*Text of User Requirement*	*SRD identifier*
AR-1-7 *essential*	The provenance system should support the following operation: Provide a simulated walkthrough on service execution flow and verify this against template workflows and/or rules governing procedures (sophistication may vary). (asked by physicians, organ transplant authority, 3rd parties (legal challenges))	SR-1-1, SR-1-2, SR-1-7
AR-1-8 *nice to have*	As an advanced feature the provenance system could support the following operation: Identify abstract derivation process of the result – based on some shared high level notions of the types of actions/content logged (e.g. having a standard view of what is an assertion, what is a decision etc.) and what follows what.	*No SR: This application specific function should be implemented by application layer software components*

A.1.2 Capability requirements

URD ID, flags, source	*Text of User Requirement*	*SRD identifier*
TR-1-1-A-1 *essential*	Recording of the following provenance information is required: Service invocation: Who accessed a particular service, when, with what input parameters (or a summary thereof) and on whose authority. 'Who' can refer to either a human or a service.	SR-1-1, SR-1-2
TR-1-1-A-2 *essential*	Recording of the following provenance information is required: Service response: Who a service sent data messages to, in response to which invocation, the content of the response (or a summary thereof). 'Who' can refer to either a human or a service.	SR-1-1, SR-1-2
TR-1-1-A-3 *nice to have*	Recording of the following provenance information would be useful: Information state: A summary of the information state in the service at the time a particular action is taken.	SR-1-1, SR-1-2
TR-1-1-A-4 *essential*	In addition to the logging of message based activities the provenance service also needs to capture "side effect" type actions (e.g. those which may not directly lead to a response message): • Carrying out an action in the real world • Recording a decision or fact	SR-1-1
TR-2-1-A *essential, critical*	"Format must be a non-proprietary format which can in principle be used with another tool (to be built if necessary) without violating IPR rules. An open standard would be best."	SR-3-2-1

URD ID, flags, source	***Text of User Requirement***	***SRD identifier***
TR-3-2 *essential*	The system should support the recording of different views on provenance information regarding to an event or an entity.	SR-1-12
TR-3-3 *essential*	The system should support the migration of provenance data among provenance repositories.	SR-1-13, SR-1-5
TR-3-4-A *essential*	On the fly recording of provenance data should be supported by the system.	*No SR: choice of the time instant for submission (immediate or delayed) depends on the application*
TR-3-6 *essential*	The system should be able to archive recorded provenance data.	SR-1-3
TR-3-7 *essential*	The system should be able to export recorded provenance data for external usage.	SR-1-5
TR-4-2 *essential*	The architecture should support the dynamic processing of provenance data, i.e. recorded provenance data should be instantly queriable even if a recording session (recording of interrelated provenance records belonging to e.g. the same workflow) is still in progress.	SR-1-8
TR-5-3 *essential*	The provenance architecture should be deployable as an integrated part of a system, as a service within the same administrative domain as the client system and as a 3rd (external) party operated service, too.	SR-1-17, SR-1-9
TR-6-1 *essential, critical*	The architecture should support a rich set of generic APIs that allow analysis and reasoning tools to be built upon.	SR-3-1-2, SR-1-9
TR-6-2	Human-computer interfaces presented by the system for analysis and reasoning should be designed to allow multilingual support.	SR-4-4

URD ID, flags, source	*Text of User Requirement*	*SRD identifier*
TR-6-5-A *essential*	Provenance information should be trackable on human-computer interfaces presented by the system at set level (e.g. database table or spreadsheet).	*No SR:* The interpretation of application specific content of recorded provenance information is not to be supported by the provenance architecture itself
TR-6-6-A *essential*	Provenance information displayed by the system on a HCI should be updatable on user request.	SR-4-1
TR-6-6-B *essential*	HCIs presented by the provenance system for provenance monitoring should support continuous monitoring, i.e. the displayed information should be updated automatically on every change as soon as possible.	SR-4-2

A.1.3 Constraint requirements

URD ID, flags, source	*Text of User Requirement*	*SRD identifier*
CR-1-1-A *essential*	Provenance recording should not impede a human entering data in real time.	SR-2-1
CR-1-2-A *essential*	Recorded provenance data should not exceed 20% of overall system record data.	SR-2-2
CR-4-1 *essential, critical*	The provenance architecture should have a configurable, fine-grained access control system over recorded provenance data.	SR-6-1
CR-4-2 *essential*	The provenance architecture should allow both automated and manual determination of access control rights on generated provenance data.	SR-6-2
CR-5-1 *essential, critical*	The provenance architecture should have good application fit, meaning: meet the basic logging needs and have additional potential for more complex questions outlined in the scenario description.	SR-1-1, SR-3-1-1, SR-3-1-2

URD ID, flags, source	*Text of User Requirement*	*SRD identifier*
CR-5-2 *essential, critical*	The provenance architecture should have the properties of cost efficiency and robustness versus an in-application hand-engineered logging system.	SR-7-1

A.2 Mapping of Software Requirements to User Requirements

SRD ID, flags	*Text of Software Requirement*	*Source (URD ID)*
Functional requirements		
SR-1-1 *essential, critical*	The provenance architecture should provide for the recording and querying of interaction and actor provenance. Source (URD ID): AR-1-1, AR-1-2, AR-1-3, AR-1-5, AR-1-6, AR-1-7, TR-1-1-A-1, TR-1-1-A-2, TR-1-1-A-3, TR-1-1-A-4, CR-5-1	*sources indicated in previous cell*
SR-1-2 *essential*	The provenance architecture should allow the retrieval of a provenance trace from the Provenance Store. Either a complete trace or a subset may be retrieved. Source (URD ID): AR-1-1, AR-1-2, AR-1-3, AR-1-5, AR-1-6, AR-1-7, TR-1-1-A-1, TR-1-1-A-2, TR-1-1-A-3	*sources indicated in previous cell*
SR-1-3 *essential*	The provenance architecture should allow the back-up of a Provenance Store to be taken. This will generally include an archiving facility that allows data within a Provenace Store to be saved for future use.	TR-3-6
SR-1-4 *essential*	The provenance architecture should allow comparisons to be made across Provenance Records within a Provenance Store with reference to particular data attributes within a Provenance Record.	AR-1-1, AR-1-6
SR-1-5 *essential*	The provenance architecture should allow the results of a query to the Provenance Store to be captured for future use. A query in this context must be specified with reference to the structure of the Provenance Store.	TR-3-3, TR-3-7

SRD ID, flags	*Text of Software Requirement*	*Source (URD ID)*
SR-1-7 *desirable*	The provenance architecture should allow a user to verify the contents of a Provenance Store against a specified set of rules. Verification in this context means that the contents of the Provenance Store meets the set of constraints expressed by the set of rules.	AR-1-1, AR-1-7
SR-1-8 *essential*	The provenance architecture should allow a user to specify a time period in the future at which a provenance query may be submitted to a Provenance Store. A scheduler will be made available that allows queries to be stored to disk, and dispatched to the store in the future.	TR-4-2
SR-1-9 *essential*	SR-1-9: The provenance architecture should allow capabilities provided by the tools to be accessible as an API. This is to allow such capabilities to be embedded within an existing application.	TR-5-3, TR-6-1
SR-1-12 *essential*	The system should support the recording of different provenance information views related to an event or an entity.	TR-3-2
SR-1-13 *essential*	The provenance architecture should support the migration of provenance data among provenance stores.	TR-3-3
SR-1-17 *essential*	The provenance architecture should be deployable as an integrated part of a system, as a service within the same administrative domain as the client system and as a 3rd (external) party operated service, too.	TR-5-3
Performance requirements		
SR-2-1 *essential*	The additional execution overhead for an application recording provenance information should be kept to a minimum.	CR-1-1-A
SR-2-2 *essential*	Storage space requirements of the provenance architecture for provenance information recording should be kept at a reasonably low level.	CR-1-2-A
Interface requirements		
SR-3-1-1 *essential, critical*	All of the functions of the provenance architecture should be accessible through its API so it can be used as an embedded component in a system.	CR-5-1
SR-3-1-2 *essential, critical*	The provenance architecture should support a rich set of published, generic APIs that allow application specific analysis and reasoning tools to be built upon.	TR-6-1, CR-5-1
SR-3-2-1 *essential, critical*	Export formats for provenance data should be non-proprietary to allow tools and applications to be built without violating IPR rules. A format based on an existing data representation standard (with special focus on XML defined by XML Schema) would be highly preferred.	TR-2-1-A
Operational requirements		
SR-4-1 *essential*	Provenance information displayed by the provenance architecture on a HCI should be updatable on user request.	TR-6-6-A

SRD ID, flags	*Text of Software Requirement*	*Source (URD ID)*
SR-4-2 *essential*	HCIs presented by the provenance architecture for displaying the contents of a Provenance Store should support continuous monitoring, i.e. the displayed information should be updated automatically on every change as soon as possible.	TR-6-6-B
SR-4-4 *essential*	Human-computer interfaces presented by the provenance tools should be designed to allow multilingual support.	TR-6-2
Security requirements		
SR-6-1 *essential, critical (myGrid)*	The provenance architecture should have a configurable access control system over the resources it provides, with a granularity that is sufficient to protect these resources.	CR-4-1
SR-6-2 *essential*	The provenance architecture should allow both automated and manual determination of access control rights.	CR-4-2
Other requirements		
SR-7-1 *essential, critical*	The provenance architecture should have the properties of cost efficiency and robustness versus an in-application hand-engineered logging system.	CR-5-2

Appendix B Detailed Test Scenario Descriptions

This chapter presents step-by-step descriptions of the three tests scenarios used for user evaluation of the system.

Each scenario is composed by:

- *Summary*: a short description of the scenario.
- *PHASE A*: the run of the transplant management scenario, which will generate the p-assertions and record them in different provenance stores.
- *PHASE B*: the execution of the tools to query and analyze the execution through the recorded p-assertions.

Some characteristics common to all three scenarios:

- **Actors:** the human actors in these scenarios are three doctors and 4 patients.

The doctors:

Name	***Username***	***Password***
Marta Sánchez Sánchez	msanchez	msanchez
Javier Vázquez Salceda	jvazquez	jvazquez
Sergio Alvarez Napagao	salvarez	salvarez

The patients:

Name	***Medical ID type***	***Medical ID***
Ramón Pérez Pérez	Catalonian Insurance Number	36347834E
Laura Gómez Ruiz	Catalonian Insurance Number	47347342F
Carlos García Quiñones	Catalonian Insurance Number	34378433B
Mr. Anderson	EU Insurance Number	12345678A

- **Organizations:** the scenarios include three hospitals and the transplant authority in Catalunya. The transplant authority is Organización Catalana de Trasplantes (OCATT). The hospitals are Hospital de Sant Pau, Hospital de la Vall d'Hebron and Hospital Clinic. The services in OCATT are authenticating doctors and applications, registering and identifying patients. The services in the hospitals are querying and updating the EHCR of a patient and other organ transplant management services.

- **Applications:** The application providing the services in OCATT is called EHCR_Auth. The applications providing the services of the hospital are called EHCR Store (EHCRS), test Medical Application (TEST_MA) and Organ Transplant Management application (OTM). OTM provides

the organ transplant management services, EHCRS provides services for querying and updating the EHCR of a patient. TEST_MA provides a GUI for testing EHCRS. EHCR_Auth, EHCRS and OTM are provenance aware applications, while TEST_MA is not. There is a tool for provenance (Tool) that helps humans to understand the content of the PS.

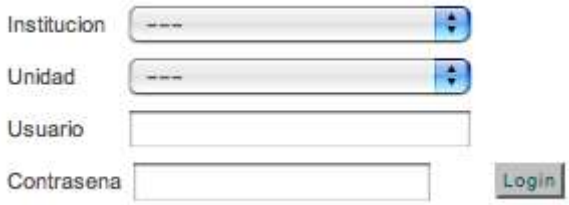
- **Initialization for all scenarios:** all applications are installed; the doctors are registered in OCATT and in every EHCR Stores; patients are not registered in OCATT; EHCR Stores, TEST_MAs and OTMs are registered in OCATT; Provenance Store is empty.

- **Important aspects of the web interface:** The scenarios include screenshots from the web interface. This web interface allows the users involved in the organ transplant management process to log all the steps of an organ transplant or extraction, from the moment when the patient enters the hospital and to the moment the organ(s) of that patient has been either implanted or rejected. Everything is recorded so that any person involved can make queries about the provenance of the data.

  Login

  The login procedure allows a user to get into the system. Each user has one or more roles and places from where he or she can connect to the OTM GUI.

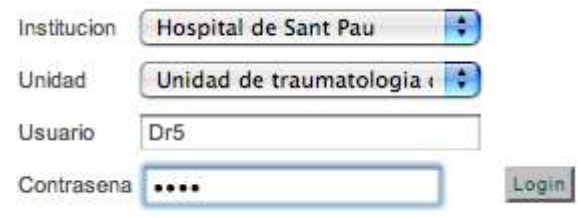
  The user opens the web interface and the login form is shown.



  This form defines four inputs: the institution from where the user is logging in (*'Institucion'*), the name of the unit (*'Unidad'*), the unique username (*'Usuario'*) and the password (*'Contraseña'*).

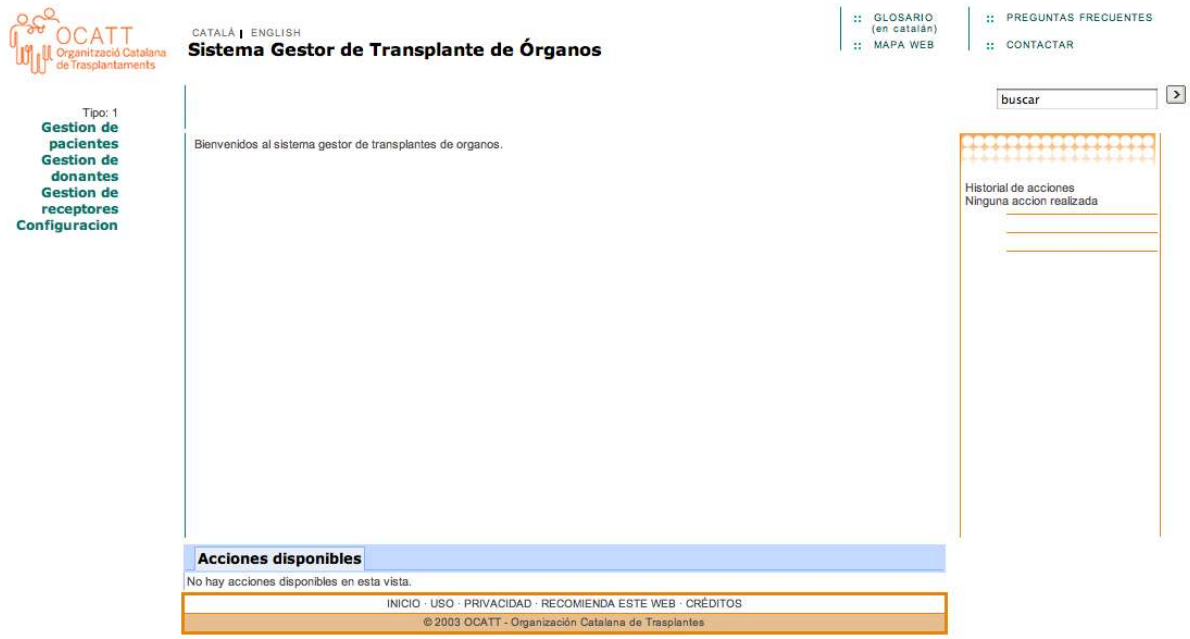
  In order to select the institution and the unit, the interface shows listboxes with the lists of choices.

  Then the username and the password are entered in their corresponding text boxes.



Main page

The main page is the shown, with the main menu displayed on the left side.

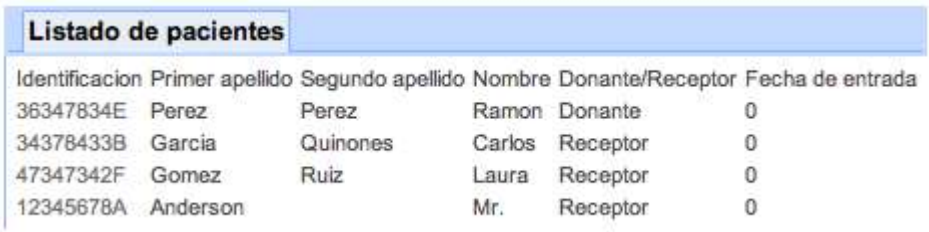


Patient List

When logged into a specific hospital institution, any user with the proper authorizations can check the list of patients being treated in that hospital unit

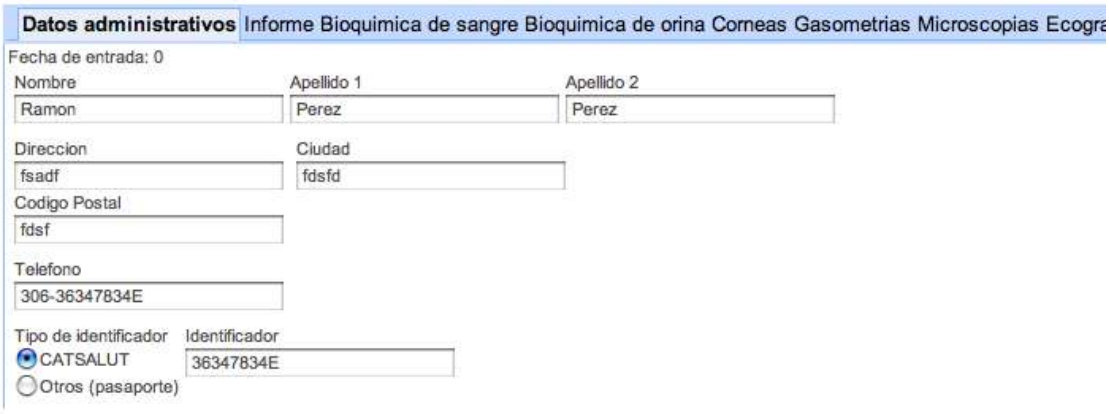
To get the list of patients, there is an option inside the menu's Patient Management section (*'Gestión de pacientes'*).

By selecting the Patient List option (*'Listar Pacientes'*), the list of patients in that hospital will be shown in the central working area of the interface.

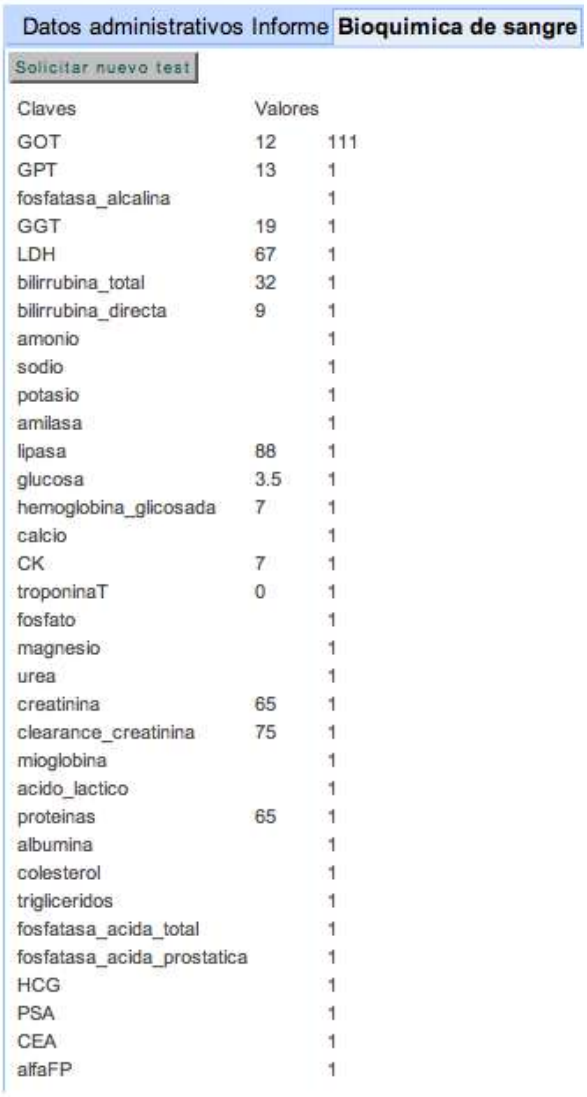


See a Patient Record and Request a Test

When the user selects a patient from the Patient List, a multipage view is presented with the patient administrative data in the front page.



The user can select among many pages, which include every type of test and additional reports.



Claves	Valores	
GOT	12	111
GPT	13	1
fosfatasa_alcalina		1
GGT	19	1
LDH	67	1
bilirrubina_total	32	1
bilirrubina_directa	9	1
amonio		1
sodio		1
potasio		1
amilasa		1
lipasa	88	1
glucosa	3.5	1
hemoglobina_glicosada	7	1
calcio		1
CK	7	1
troponinaT	0	1
fosfato		1
magnesio		1
urea		1
creatinina	65	1
clearance_creatinina	75	1
mioglobina		1
acido_lactico		1
proteinas	65	1
albumina		1
colesterol		1
trigliceridos		1
fosfatasa_acida_total		1
fosfatasa_acida_prostatica		1
HCG		1
PSA		1
CEA		1
alfaFP		1

When selecting a test, the first thing the user can see is a button that allows him/her to request a new test of that type to the nearest laboratory. If previous tests have already been made, they are listed in a table under the button.

As soon as the test has been fulfilled by the receiver laboratory, its results can be seen in the same table, in a new column.

B.1 SCENARIO S1: Start of a medical history, and patient record availability from one hospital to another

This scenario shows how simple medical events are recorded in the provenance store and how this events create a medical process – the medical history or a case – of a patient.

B.1.1 Summary

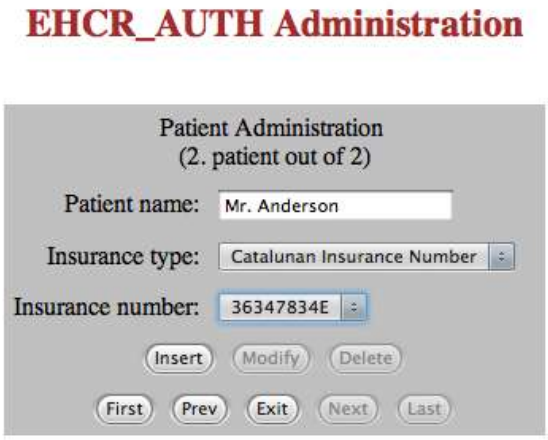
In this scenario we show how a medical history and EHCR started, updated and queried. The patient is called Mr. Anderson. His medical history starts in phase A / Step 1 (S1.1), when he is registered in OCATT with his national insurance number. In phase A / Step 2 (S1.2) his EHCR is created in Hospital de la Vall d'Hebron and updated in Hospital Clinic. In phase B / Query 1 (Q1.1) Mr. Anderson's EHCR is queried in Hospital de Sant Pau. In phase B / Query 2 (Q1.2) Mr. Anderson's medical history is queried using the Tool of provenance.

B.1.2 PHASE A: the scenario run

S1.1 Start the medical history of Mr. Anderson

- User ehcrauth logs into patient administration site of OCATT.

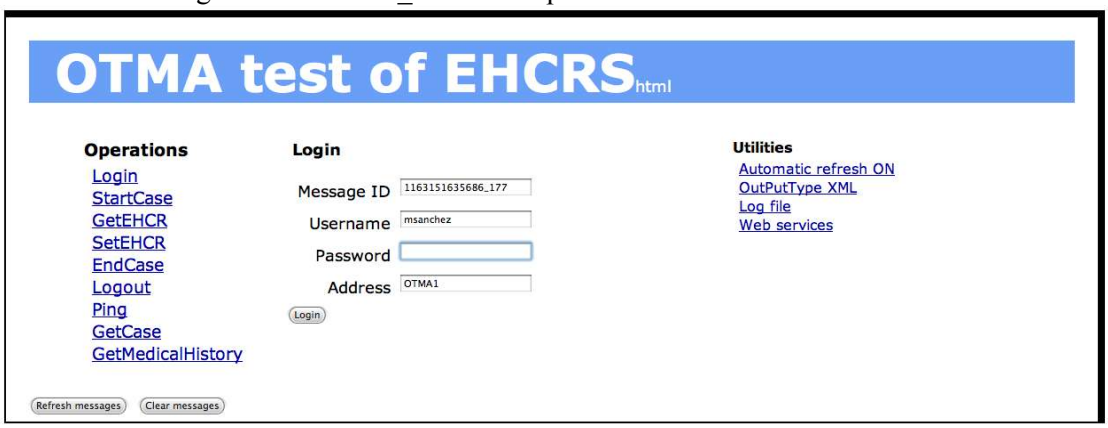
- He/she registers Mr. Anderson as a new patient with Catalonian Insurance Number 363478234E.



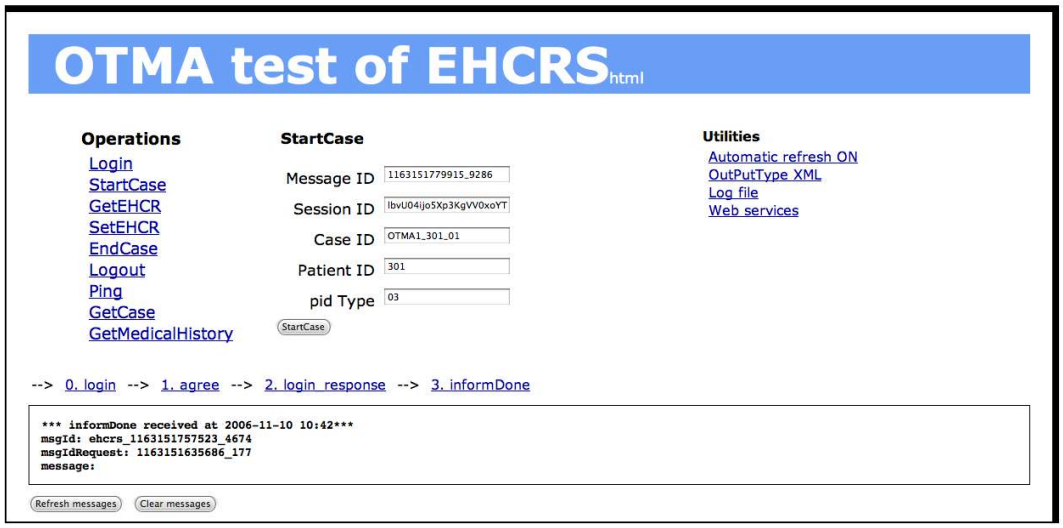
- This process is documented in the provenance store.

S1.2 Treat Mr. Anderson

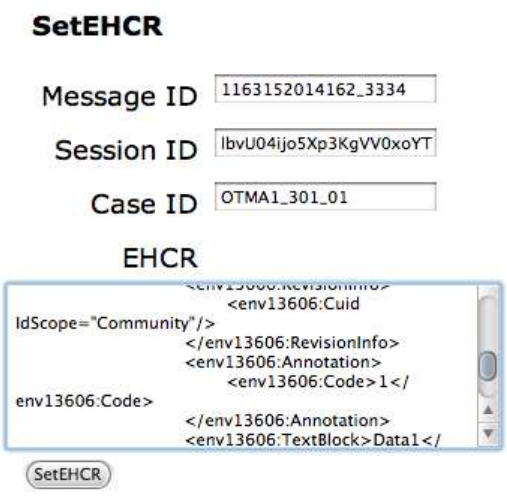
- User msanchez logs into the TEST_MA of Hospital de la Vall d'Hebron.



- She opens case 03_301_01 for Mr. Anderson.



- Then she updates Mr. Anderson's electronic healthcare record.



- User msanchez logs out from the TEST_MA at Hospital de la Vall d'Hebron.

- The process is repeated with jvazquez, TEST_OTM of Hospital Clinic, case 03_301_02 and a different content of EHCR.

Some important things to remark about this part of the scenario:

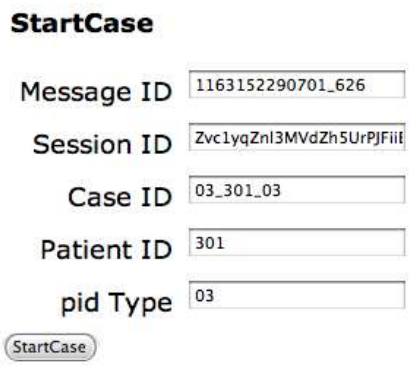
- When msanchez logs in the OCATT authenticates both the doctor and the TEST_OTM she uses.
- When the doctor opens a case, OCATT connects this event to the first event of Mr. Anderson's medical history in the provenance store, namely when he was registered in OCATT.
- When msanchez updates the EHCR this event is connected to the opening case event in the provenance store.

B.1.3 PHASE b: querying the Provenance store

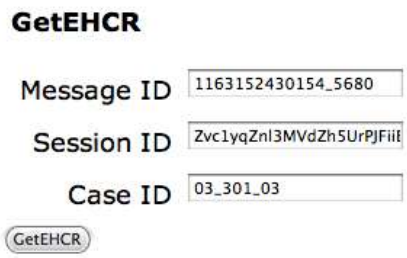
Q1.1 Query Mr. Anderson's whole EHCR from EHCRS3

- User salvarez logs into TEST_MA of Hospital de Sant Pau.

- He opens case 03_301_03 for Mr. Anderson.



- Then he queries the whole EHCR of Mr. Anderson; finds nothing locally, some from Hospital de la Vall d'Hebron and some from Hospital Clinic.



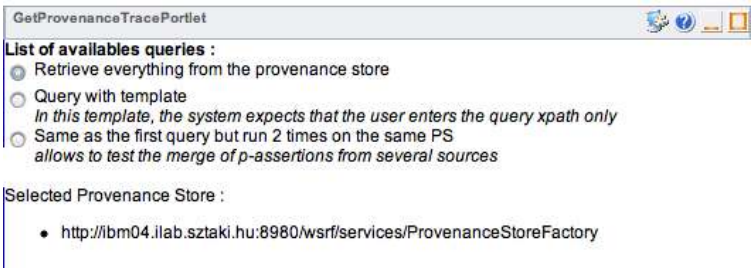
- Finally user salvarez logs out from TEST_MA of Hospital de Sant Pau.

When salvarez queries the EHCR of Mr. Anderson the system queries medical history of the patient from the provenance story and tries to figure out where the EHCR was updated analyzing the process documentation. Then the system queries the other hospitals following the ENV13606 standard.

Q1.2 Query Mr. Anderson's medical history from provenance store

- User provenance logs into the tool of provenance.

- The user queries the provenance store.

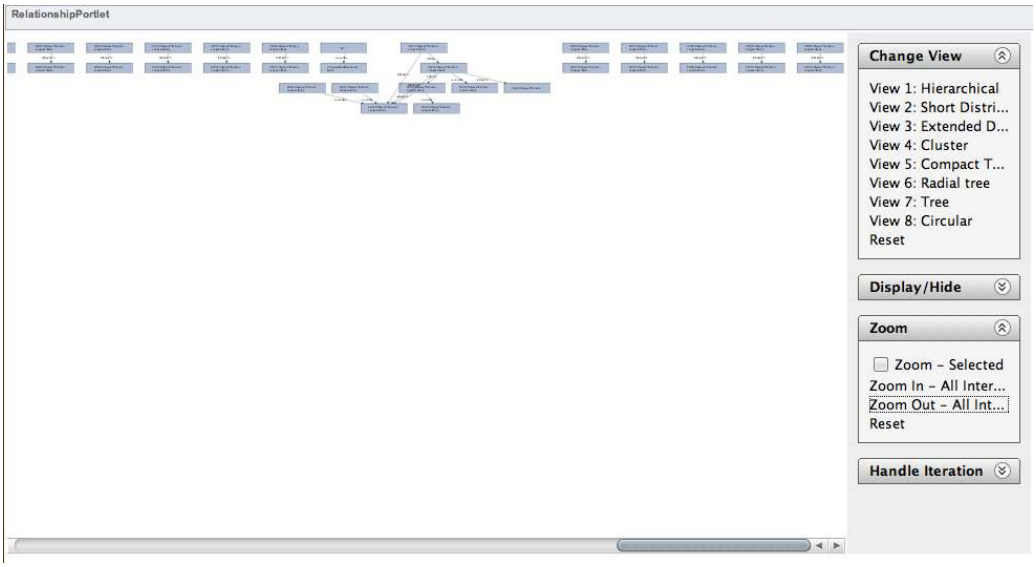


- Then he/she uses the text and graphical tool to analyze the medical history or a case.

111 p-record(s) extracted, containing :

- 172 interaction p-assertion(s)
- 176 actor state p-assertion(s)
- 142 relationship p-assertion(s)

Passertion ID :	From :	To :
http://uniqueId/1162492563195	ehcrauth	EHCRS2
http://uniqueId/1162492147477	ehcrauth	EHCRS2
http://uniqueId/1163151968307	EHCRS1	EHCRS3
http://uniqueId/1163148565513	EHCRS1	ehcrauth
http://uniqueId/1162492161336	EHCRS1	ehcrauth
http://uniqueId/1163148556547	EHCRS1	OTM:CollectPatientData
http://uniqueId/1162491901187	OTMA2	EHCRS2
http://uniqueId/1162491907981	EHCRS2	OTMA2
http://uniqueId/1163151935019	EHCRS1	ehcrauth
http://uniqueId/1162491903828	ehcrauth	EHCRS2
http://uniqueId/1163151960158	EHCRS1	ehcrauth
http://uniqueId/1163152430839	OTMA1	EHCRS1
http://uniqueId/1163162342679	adminGUI	ehcrauth
http://uniqueId/1162492288270	EHCRS2	ehcrauth
http://uniqueId/1162492138946	EHCRS2	OTMA2
http://uniqueId/1162492252875	ehcrauth	EHCRS3
http://uniqueId/1163152246187	ehcrauth	EHCRS1
http://uniqueId/1163151738946	OTMA1	EHCRS1
http://uniqueId/1162492150744	EHCRS2	EHCRS1
http://uniqueId/1163152465567	ehcrauth	EHCRS3
http://uniqueId/1162492196325	EHCRS2	EHCRS3
http://uniqueId/1163152461250	EHCRS1	EHCRS3
http://uniqueId/1163148571995	EHCRS1	OTM:CollectPatientData
http://uniqueId/1163152366633	EHCRS1	OTMA1
http://uniqueId/1162492164267	ehcrauth	EHCRS1
http://uniqueId/1162492568082	EHCRS2	OTMA2
http://uniqueId/1163152244482	EHCRS1	ehcrauth



- Finally user provenance logs out from the provenance tool.

B.2 SCENARIO S2: Patient record available at Hospital A, offer from Hospital A accepted by first contacted hospital (Hospital B)

This scenario represents a transplant management case when everything goes smoothly (an almost "ideal" case).

B.2.1 Summary

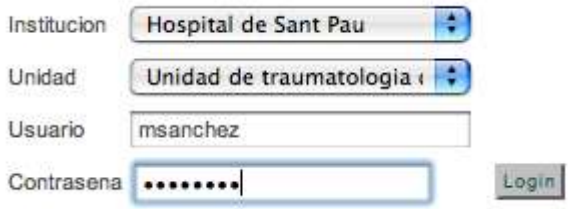
There is a patient A1 in hospital A that becomes potential donor; after getting the results from the tests a donation decision states that the heart and the liver will be donated; the offer is sent to the OTA, which forwards it to the first hospital candidate (Hospital B) which accepts both offers. An

extraction team from Hospital B travels to Hospital A and, after extraction and close examination of patient A1 organs, decides that the liver is in no good condition to be implanted, but the heart is indeed in good condition. Extraction team returns to Hospital B and then implants the organ to patient B2.

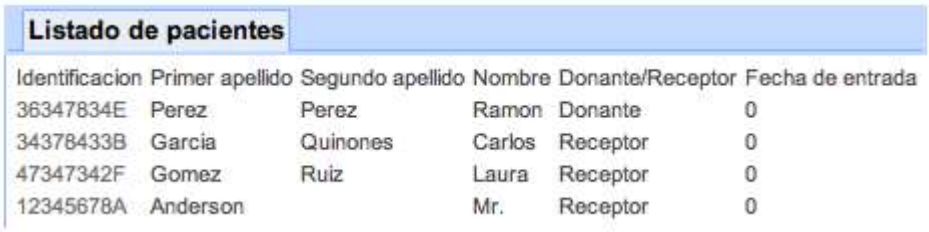
B.2.2 PHASE A: the scenario run

S2.1. Patient B2 in Hospital B registered as heart recipient in recipient list

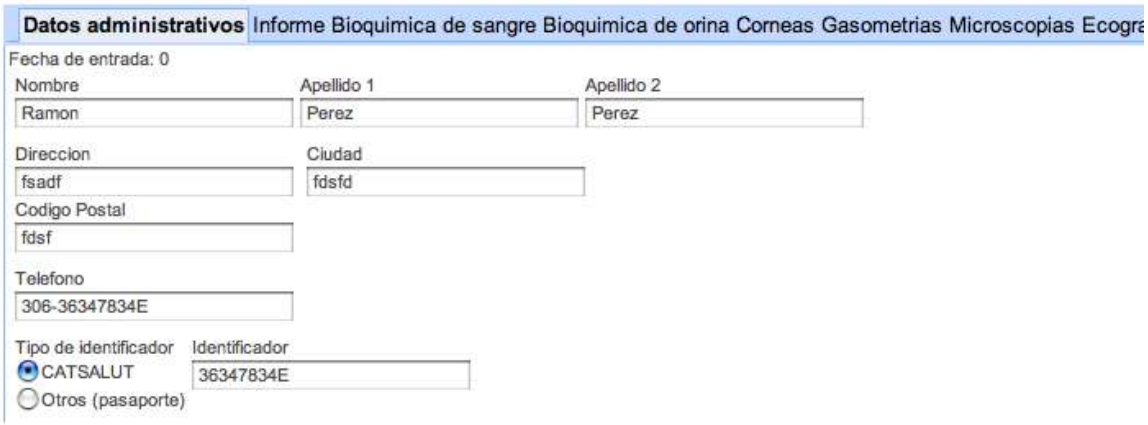
- Management Staff Member B in Hospital B logs in the system.



- Management Staff Member B in Hospital B opens the patient list of Hospital B in the web interface(See ***Patient List***).
- The web interface shows the patient list of Hospital B to Management Staff Member B.

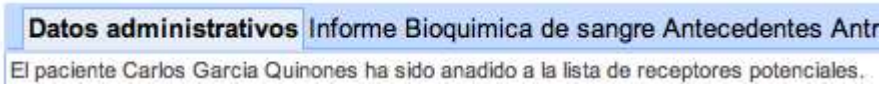


- Management Staff Member B selects Patient B2 in the web interface. To do so, the user clicks on the Identification number of Patient B2.



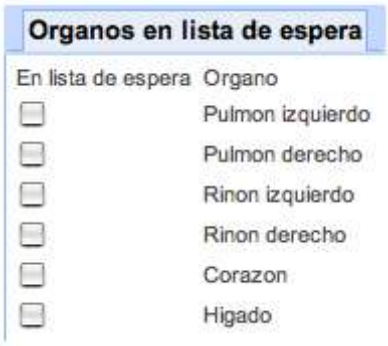
- The web interface shows the full record of Patient B2 to Management Staff Member B.
- Management Staff Member B clicks the "Give Potential Recipient Status" button ('*Receptor Potencial*') in the Patient B2 record screen, located at the Action Button Bar.

- Once clicked, if the action is successful, the user can see the confirmation.

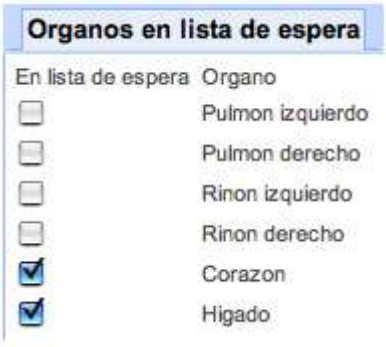


- The Action Button Bar changes with the new potential recipient status. One of the new options that appears is the "Manage Waiting List" one (*'Gestionar lista de espera'*). Management Staff Member B selects the "Manage Waiting List" button in the Patient B2 record screen.

- The web interface shows the list of organs for Patient B2.

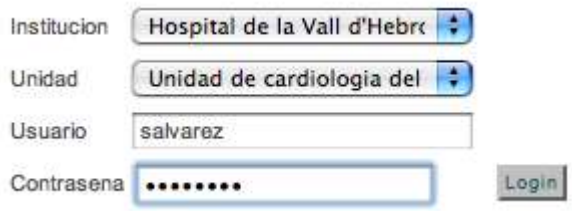


- Management Staff Member B selects heart (*'Corazón'*) and liver (*'Hígado'*).

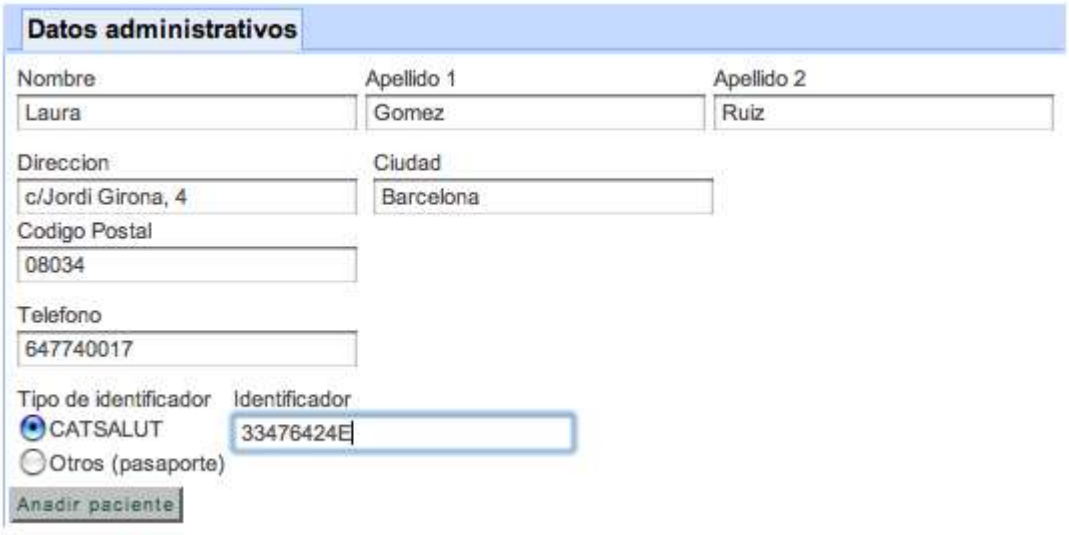


S2.2. A potential donor patient A1 appears in hospital A

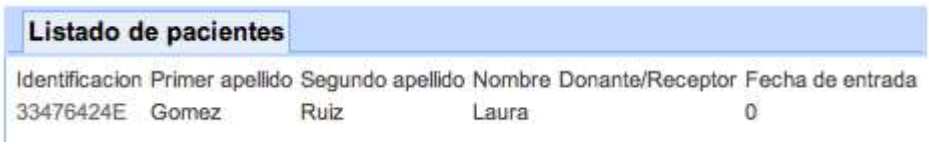
- Doctor A in Hospital A logs in the system.



- Doctor A in Hospital A registers a new Patient A1 in the web interface. To do so the doctor goes to the patient section of the main menu and selects the "Add a new patient" option (*'Añadir paciente'*).
- Then the doctor can see an empty form for the administrative data. The doctor fills the form and clicks on the "Add patient" button (*'Añadir paciente'*).



- Once the doctor has clicked on the button, he waits for a few seconds and then is returned to the patient list, with the new patient already added.

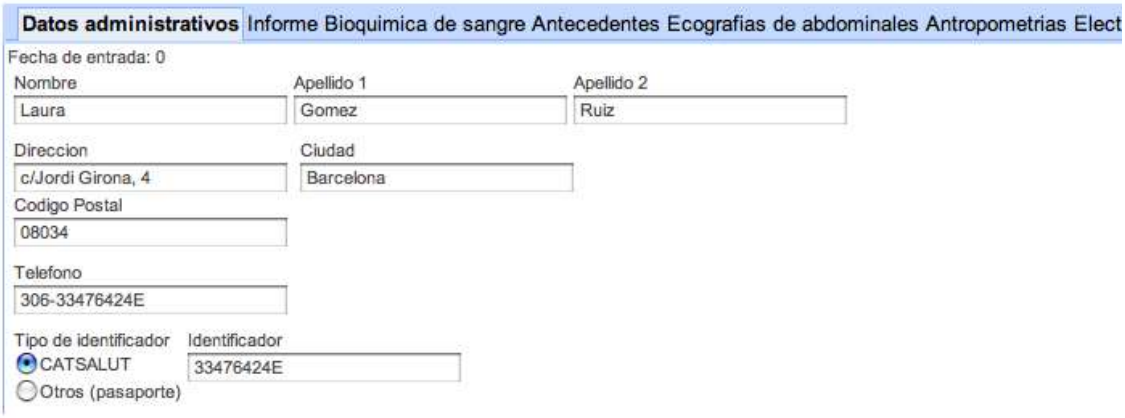


S2.3 Query to EHCRS to see if there is a patient record for patient A1

- Doctor A in Hospital A refreshes Patient A1 information in the web interface. To do so he clicks on the patient's Identification Number.

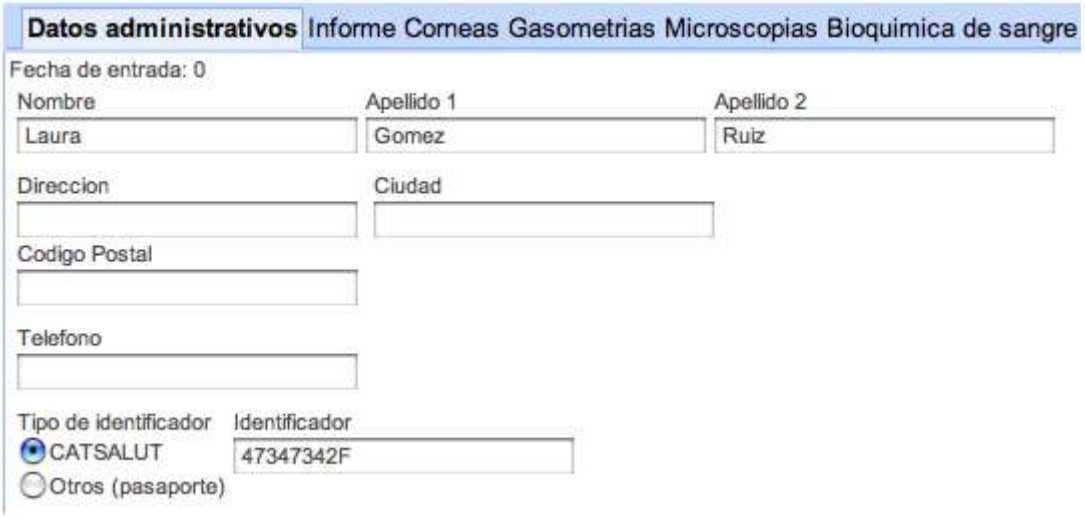
S2.4. The patient record was already present at the EHCR-a

- The web interface updates the record of Patient A1 for Doctor A in Hospital A. The doctor can see now the full history of the patient.



S2.5. A staff member from Hospital A declares patient A1 as potential donor

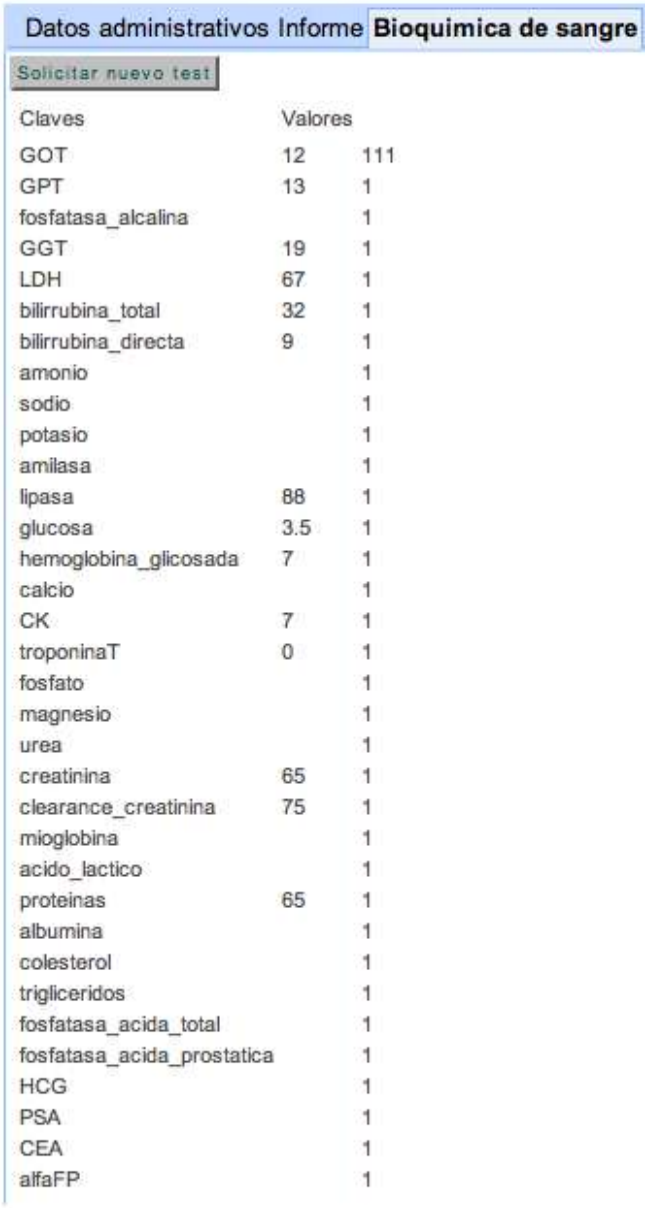
- Management Staff Member A in Hospital A opens the patient list of Hospital A in the web interface (see **Patient List**).
- The web interface looks for the patient list of Hospital A in the EHCRS A.
- The web interface shows the patient list of Hospital A to Management Staff Member A.
- Management Staff Member A selects then Patient A1 in the web interface.
- The web interface shows the full record of Patient A1 to Management Staff Member A.



- Management Staff Member A selects the "Give Potential Donor Status" button (*'Donante Potencial'*) in the Patient A1 record screen, located at the Action Button Bar.

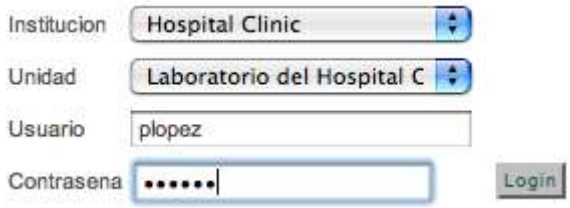
S2.6 The staff member from Hospital A requests a blood test to Lab A

- Management Staff Member A in Hospital A looks at the blood test history of Patient A1 in the web interface
- Management Staff Member A in Hospital A requests a test for Patient A1 in the web interface. To do so the doctor clicks on the "Request Test" button (*'Solicitar nuevo test'*) at the top of the test screen.



Claves	Valores	
GOT	12	111
GPT	13	1
fosfatasa_alcalina		1
GGT	19	1
LDH	67	1
bilirrubina_total	32	1
bilirrubina_directa	9	1
amonio		1
sodio		1
potasio		1
amilasa		1
lipasa	88	1
glucosa	3.5	1
hemoglobina_glicosada	7	1
calcio		1
CK	7	1
troponinaT	0	1
fosfato		1
magnesio		1
urea		1
creatinina	65	1
clearance_creatinina	75	1
mioglobina		1
acido_lactico		1
proteinas	65	1
albumina		1
colesterol		1
trigliceridos		1
fosfatasa_acida_total		1
fosfatasa_acida_prostatica		1
HCG		1
PSA		1
CEA		1
alfaFP		1

- At some moment, Lab Staff Member A in Lab A of Hospital A will read the demand in the queue, in the web interface.



- Once logged, the Lab Staff Member A checks the Test Request List (*'Listado de peticiones de test'*) in the Test Management section (Gestión de Tests) of the main menu (Note: Test Management is only available for Lab Staff Members).
- The Lab Staff Member can see the list of the latest demanded tests.

Listado de peticiones de test

Identificador de test	Identificador de paciente	Acabado	Fecha inicio	Fecha final	Institucion
168002925	Py6x7pBB3Lg=	Si	1160187497745	1160192823824	Hospital de Sant Pau
1954070591	46962871E	Si	1160202170859	1160202203369	Hospital de Sant Pau
1321879101	46962871E	Si	1160202231029	1160202254191	Hospital de Sant Pau
1761317462	FE3Vo1DDblg=	Si	1160211301664	1160211326629	Hospital de Sant Pau
1542086776	FE3Vo1DDblg=	Si	1160213051545	1160213696366	Hospital de Sant Pau
701941894	FE3Vo1DDblg=	Si	1160213749373	1160213763979	Hospital de Sant Pau
1253521070	sadffa	Si	1160365108881	1160365196716	Hospital de Sant Pau
1527939601	sadffa		1160552114624	0	Hospital de Sant Pau
1598092898	47347342F		1162273760006	0	Hospital de Sant Pau
1951512169	47347342F		1162273773426	0	Hospital de Sant Pau
1586974207	47347342F		1162273799384	0	Hospital de Sant Pau

S2.7. The staff member from Hospital A requests a serology test to Lab A

*(Same as **S2.6**)*

- Management Staff Member A in Hospital A looks at the serology test history of Patient A1 in the web interface.
- Management Staff Member A in Hospital A selects the “Request Test” option of Patient A1 in the web interface.
- At some moment, Lab Staff Member A in Lab A of Hospital A will read the demand in the queue, in the web interface.
- A Lab Staff Member A in Lab A will log eventually in the system.

S2.8. The staff member from Hospital A requests a HLA test to Lab D (external Lab)

*(Same as **S2.6**)*

- Management Staff Member A in Hospital A looks at the HLA test history of Patient A1 in the web interface.
- Management Staff Member A in Hospital A selects the “Request Test” option of Patient A1 in the web interface.
- At some moment, Lab Staff Member D in Lab D will read the demand in the queue, in the web interface.

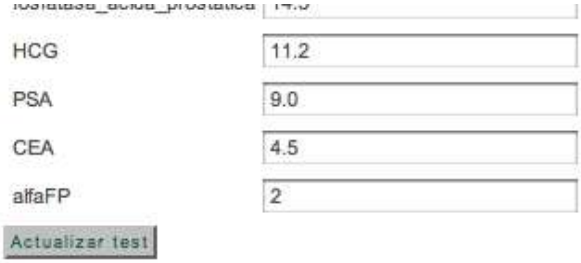
S2.9. Serology test result from Lab A arrives to Hospital A

- Lab Staff Member A in Hospital A updates the test record for the serology test of Patient A1 in the web interface (see **S2.10**).

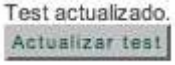
S2.10. Blood test result from Lab A arrives to Hospital A

- Lab Staff Member A in Hospital A updates the test record for the blood test of Patient A1 in the web interface. To do so, the Lab Staff Member clicks on the test identifier (at the Test List) to open its empty form.

- The Lab Staff Member fills the form with the results of the test, and then clicks on the update button ('*Actualizar test*') at the end of the page.



- Once submitted, the Lab Staff Member waits a few seconds and then receives confirmation.



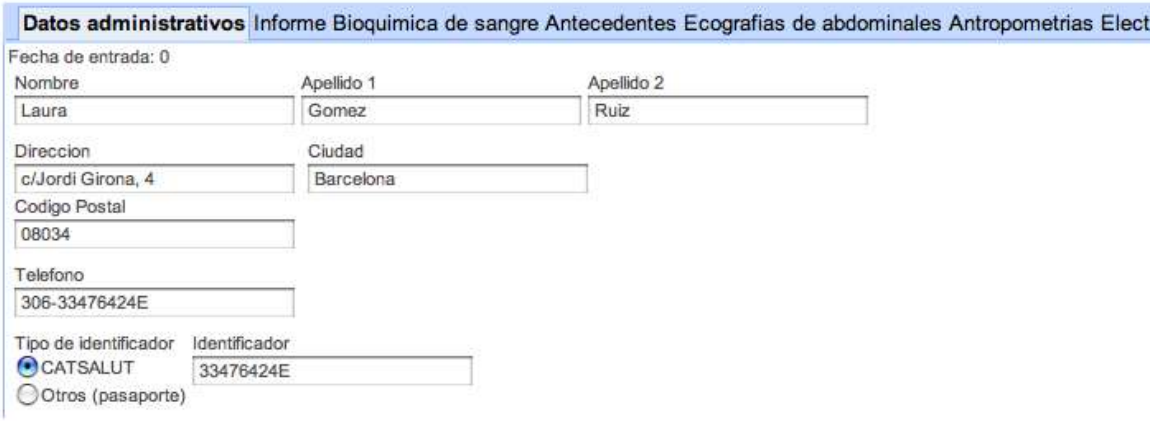
S2.11. HLA test result from Lab D arrives to Hospital A

- Lab Staff Member D in Lab D updates the test record for the HLA test of Patient A1 in the web interface (see **S2.10**).

S2.12 Decision of donation done: patient A1's heart and liver, supported by EHCR data and all 3 tests

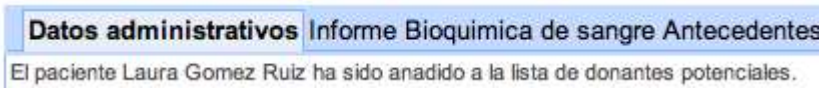
- Doctor A in Hospital A opens the patient list of Hospital A in the web interface (see **Patient List**).
- The web interface shows the patient list of Hospital A to Doctor A.

- Doctor A selects Patient A1 in the web interface. To do so, the doctor clicks on the Identification Number of Patient A1. The web interface shows the full record of Patient A1 to Doctor A



- Doctor A selects the "Give Donor Status" button (*'Donante Potencial'*) in the Patient A1 record screen.

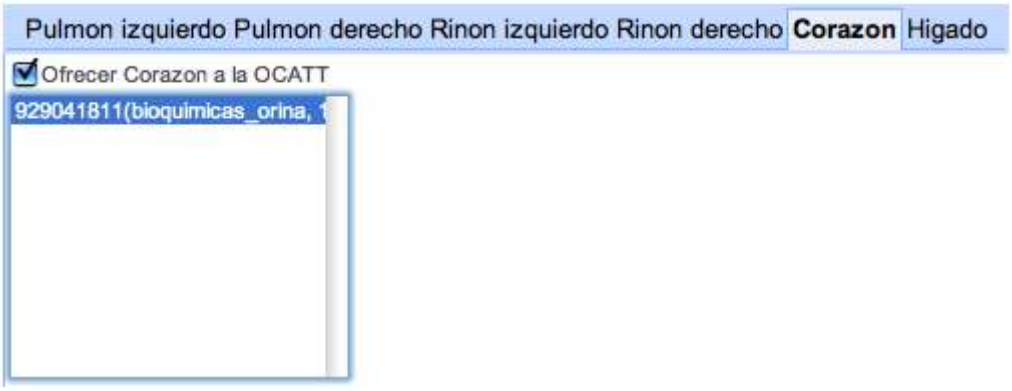
- The doctor can see the confirmation message.



- The Action Button Bar has changed. The doctor clicks now on the "Offer to OCATT" button ('*Ofertar a la OCATT*').

- The web interface shows the list of organs to Doctor A. The list of organs is presented in separate pages. Each page has a checkbox to confirm the offer of that specific organ, and a list of the last tests is provided to support the basis of the decision.

- Doctor A selects heart (*'Corazón'*) and liver (*'Hígado'*)in the web interface.
- The web interface shows the list of tests made for Patient A1, ordered by date. Doctor A selects the 3 latest tests made.

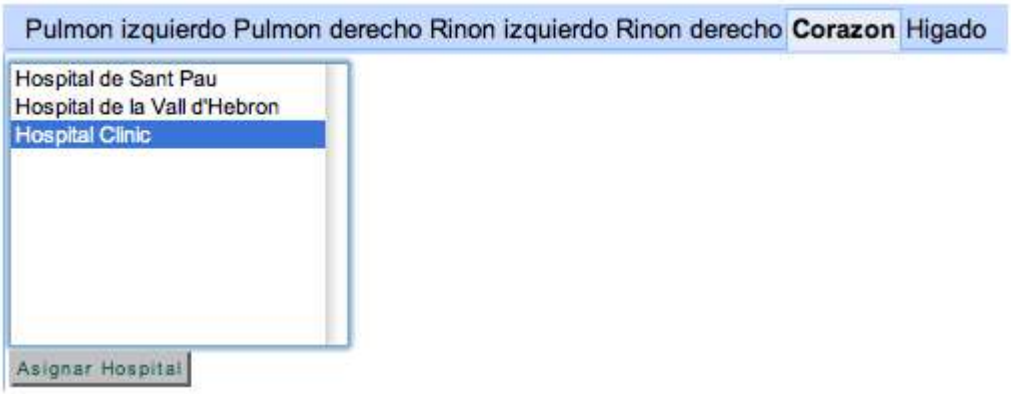


S2.13. OTA receives the donation offers and decides where to send the offers: both donation offers sent from OTA to Hospital B

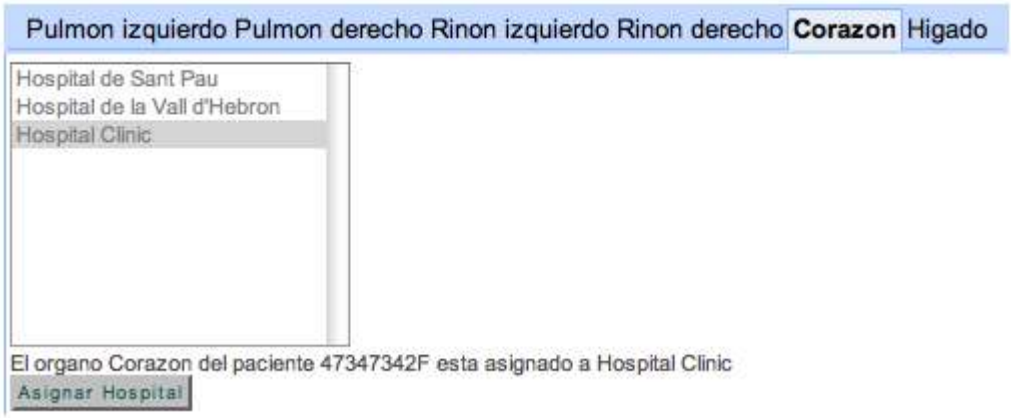
- The offers appears in the OTA interface.

- The user selects the heart offer ('*Corazón'*).

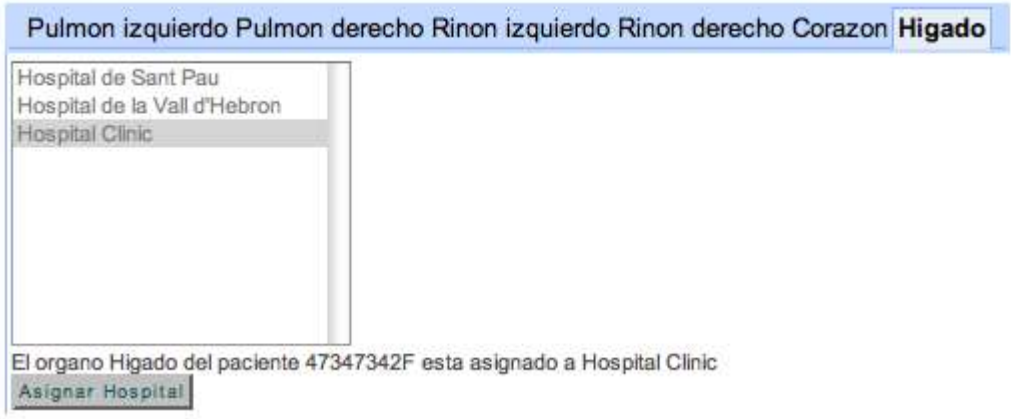
- The list of hospitals waiting for a heart appears on screen.



- The user selects 'Hospital Clinic' as destination hospital.



- The user selects then the liver offer. The list of hospitals waiting for a liver appears on screen.
- The user selects also 'Hospital Clinic' as destination hospital.



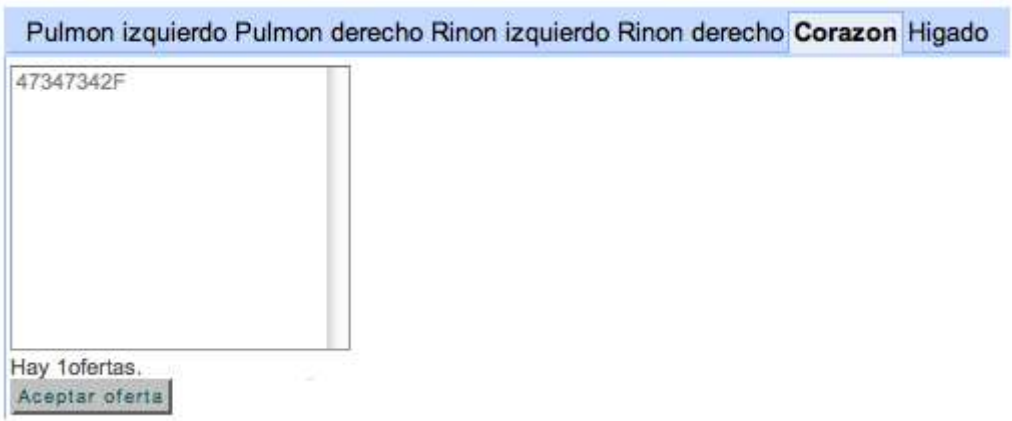
S2.14. Message to OTA: Hospital B accepts heart offering

- A Doctor or a Management Staff Member in Hospital B selects the “Recipients Management” section (*'Gestion de receptores'*) in the main menu, and then clicks on “Manage Waiting List” (*'Gestionar la lista de espera'*).

- The user can see a list of the recipients being treated in Hospital B.

- For each recipient, the user can select an organ from the list of demanded organs.

- The user selects the heart (*'Corazón'*). He can see now the list of offers received from the OTA.



- The user selects the Identification Number of the donor and clicks on "Accept Offer" (*'Aceptar oferta'*). He receives a confirmation message.

S2.15 Message to OTA: Hospital B accepts liver offering

- A Doctor or a Management Staff Member in Hospital B reads the offer of a liver in the web interface and selects the "Accept Offer" option (see **S2.14**).

S2.16. Message to OTA + Extraction report by team from Hospital B: patient A1's heart accepted for donation

- Doctor B in Hospital A logs in the web interface (see **Login**).
- Doctor B in Hospital A opens the patient list of Hospital A in the web interface.
- The web interface shows the patient list of Hospital A to Doctor B.
- Doctor B selects Patient A in the web interface.
- The web interface shows the full record of Patient A to Doctor B.
- Doctor B selects the "Extraction Report" in the Patient A record screen.
- The web interface shows a list of the organs donated by Patient A.
- Doctor B selects Heart from the list.
- The web interface shows a form for the Extraction Report to Doctor B.
- Doctor B fills the form, accepting the donation, in the web interface.

S2.17. Message to OTA + Extraction report by team from Hospital B: patient A1's liver rejected for donation – physical damage

- Doctor B in Hospital A logs in the web interface.
- Doctor B in Hospital A opens the patient list of Hospital A in the web interface.
- The web interface shows the patient list of Hospital A to Doctor B.
- Doctor B selects Patient A in the web interface.
- The web interface shows the full record of Patient A to Doctor B.
- Doctor B selects the "Extraction Report" in the Patient A record screen.
- The web interface shows a list of the organs donated by Patient A.
- Doctor B selects Liver from the list.
- The web interface shows a form for the Extraction Report to Doctor B.
- Doctor B fills the form, rejecting the donation, in the web interface.

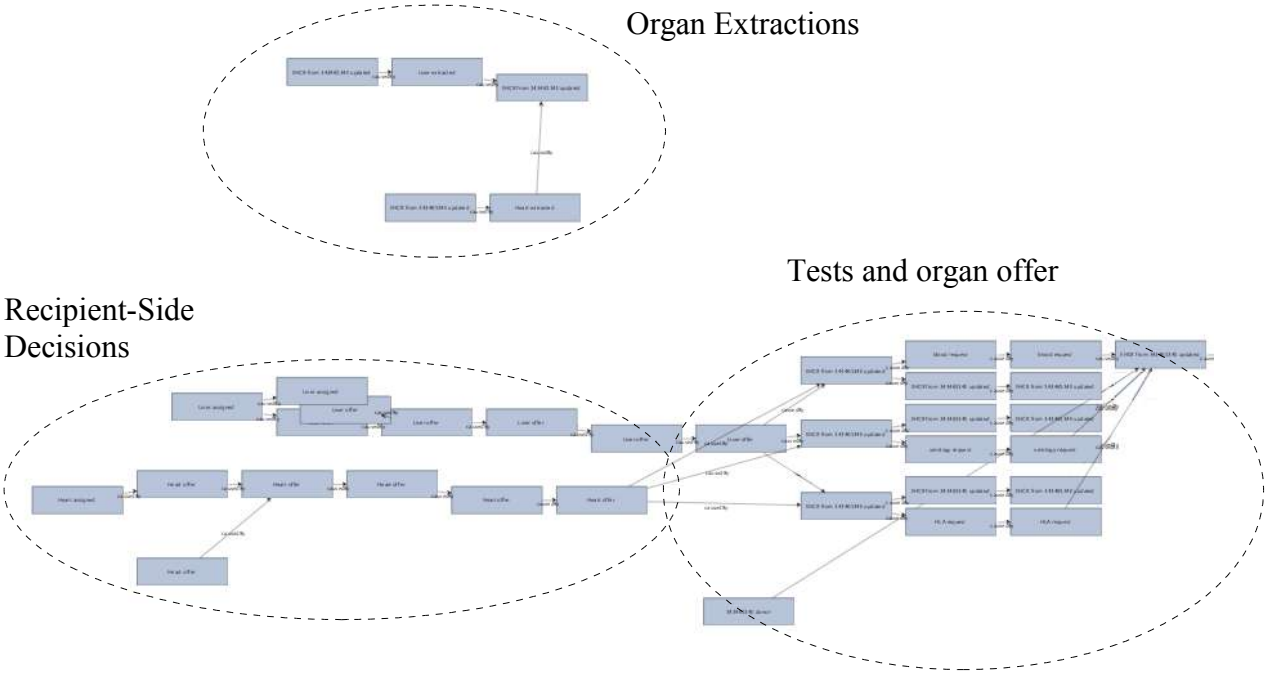
S2.18. Message to OTA + Implantation report by team from Hospital B: heart implanted to patient B2.

- Doctor B in Hospital B logs in the web interface.
- Doctor B in Hospital B opens the patient list of Hospital B in the web interface.
- The web interface shows the patient list of Hospital B to Doctor B.
- Doctor B selects Patient B2 in the web interface.
- The web interface shows the full record of Patient B2 to Doctor B.
- Doctor B selects the "Implant Report" in the Patient B2 record screen.
- The web interface shows a list of the organs being received by Patient B2.
- Doctor B selects Heart from the list.
- The web interface shows a form for the Implant Report to Doctor B.
- Doctor B fills the form in the web interface.

B.2.3 PHASE b: querying the Provenance stores

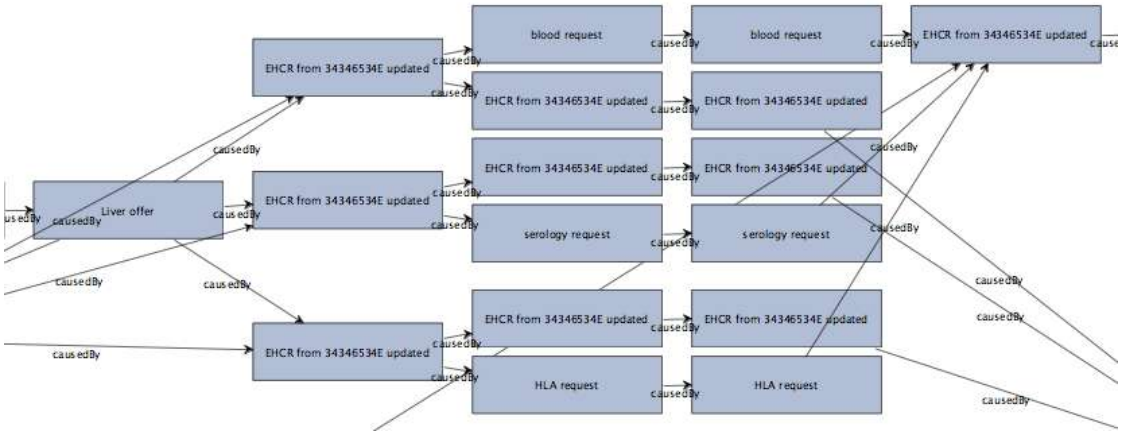
Q2.1: Obtain all events related to Patient A1

- The user selects the Patient A1 from the patient list, in the web interface.
- The web interface retrieves the data of Patient A1.
- The full record of Patient A1 is shown to the user.
- The user selects the option "Mark patient for analysis" on the action toolbar.
- The web interface creates a copy of the tools Setup Protocol files, loading the queries for a patient and the provenance store location.
- The user selects "Event Analyzer" on the main menu.
- The tool portal is shown in the main frame.
- The user selects the Query portlet and chooses "Obtain all events related to Patient A1".
- The visualization tool is shown to the user. In this case the user obtains the part of the workflow related directly with Patient A1.

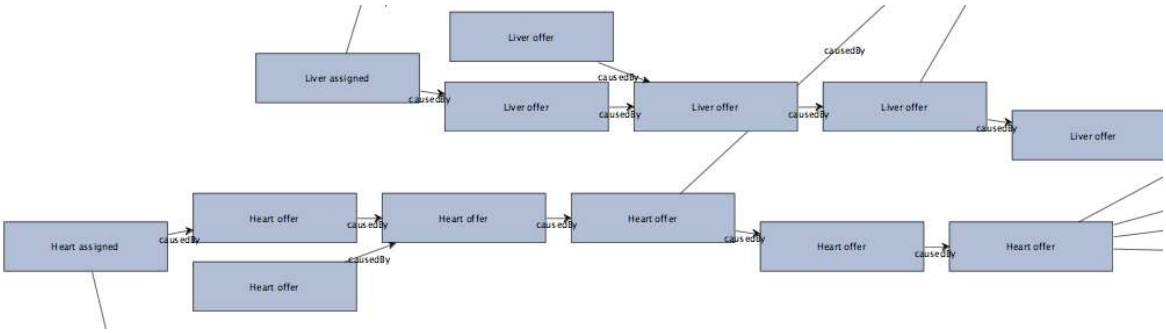


As a result of this query applied to the provenance data generated in the scenario, the doctor can identify some specific parts of the process in the diagram.

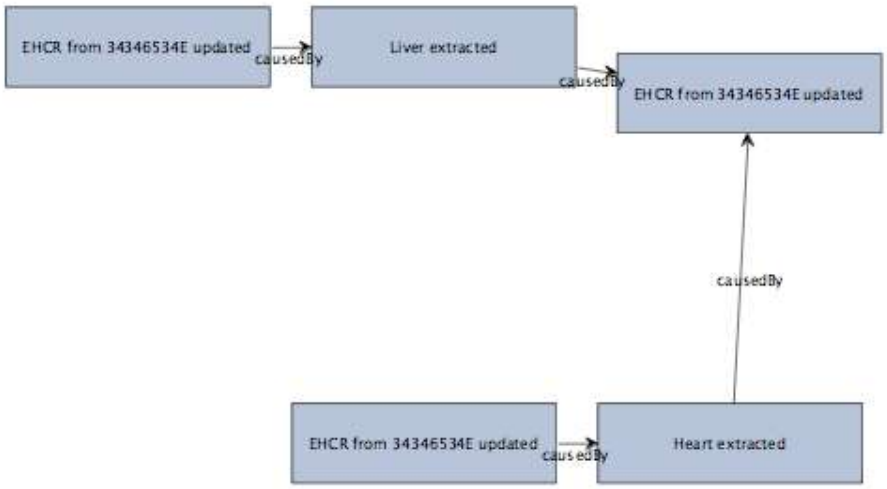
- Tests and organ offer: in this section we can see the tests carried out at the donor side and the final decision for donation, on the left.



- Recipient-Side Decisions: in this section we can see the propagation of the heart offer through the system until both the heart and the liver are assigned.



- Organ extraction: these events represent the organ extraction procedures.



Q2.2: Obtain the list of users that have registered events related to Patient B2

- The user selects the Patient B2 from the patient list, in the web interface.
- The web interface retrieves the data of Patient B2.
- The full record of Patient B2 is shown to the user.
- The user selects the option "Mark patient for analysis" on the action toolbar.
- The web interface creates a copy of the tools Setup Protocol files, loading the queries for a patient and the provenance store location.
- The user selects "Event Analyzer" on the main menu.
- The tool portal is shown in the main frame.
- The user selects the Query portlet and chooses "Obtain all users with events registered for Patient B2".
- The text visualization tool is shown to the user. The user, in this case, will see a text table with a list of users (*'Usuario'*) and the timestamps.

Usuario	msanchez	salvarez	ktamas	msanchez	jvazquez
Timestamp	1162563085343	1162563128422	1162563219243	1162563255148	1162563170097

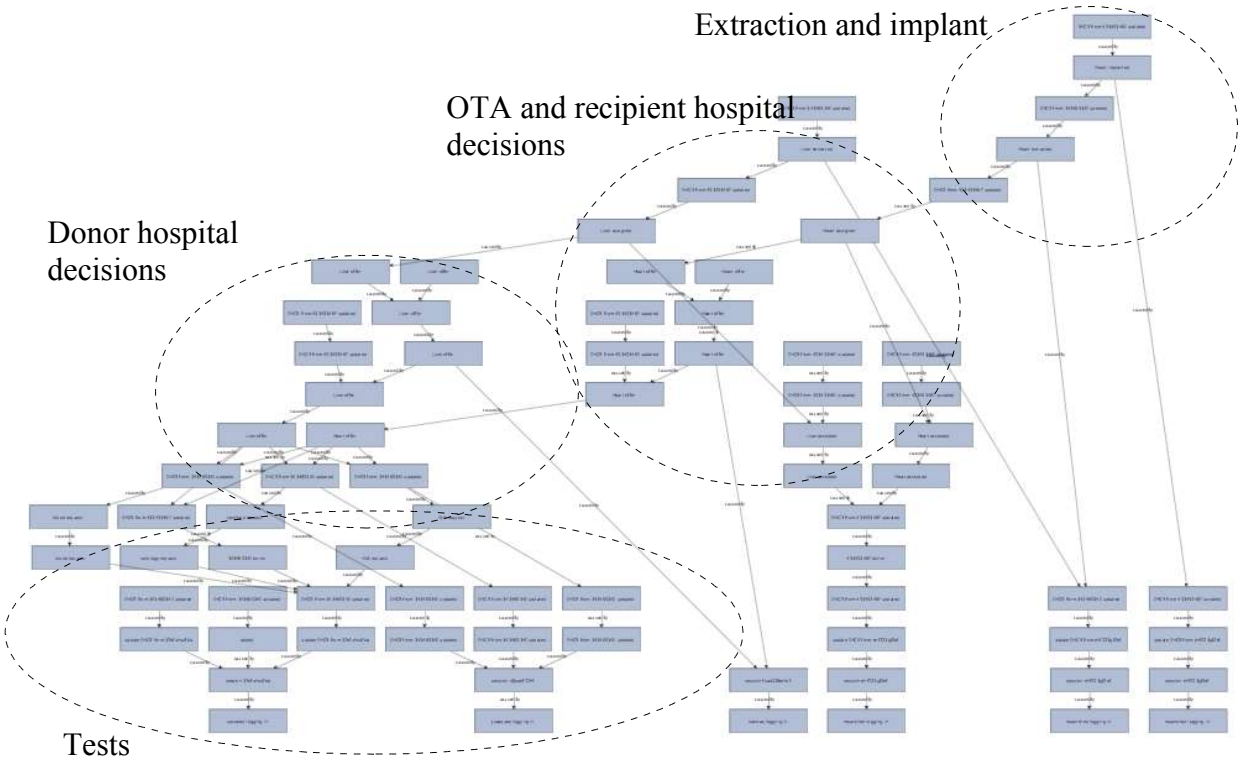
This query does not have a graphical interpretation. The user who executes this query can see a list of the users that have interacted with Patient A1 or with her data in some way. The list can have repeated users if they have used more than a session during the scenario case.

This list shows two pieces of data for each user session: the username used in the login procedure, and the time stamp. Current version of the system shows the timestamps in a special format used by Unix systems: number of milliseconds since January 1st, 1970. This will be fixed in next versions of

the OTM system. Approximately the timestamps in this example are between 2pm and 3pm of November 3rd, 2006.

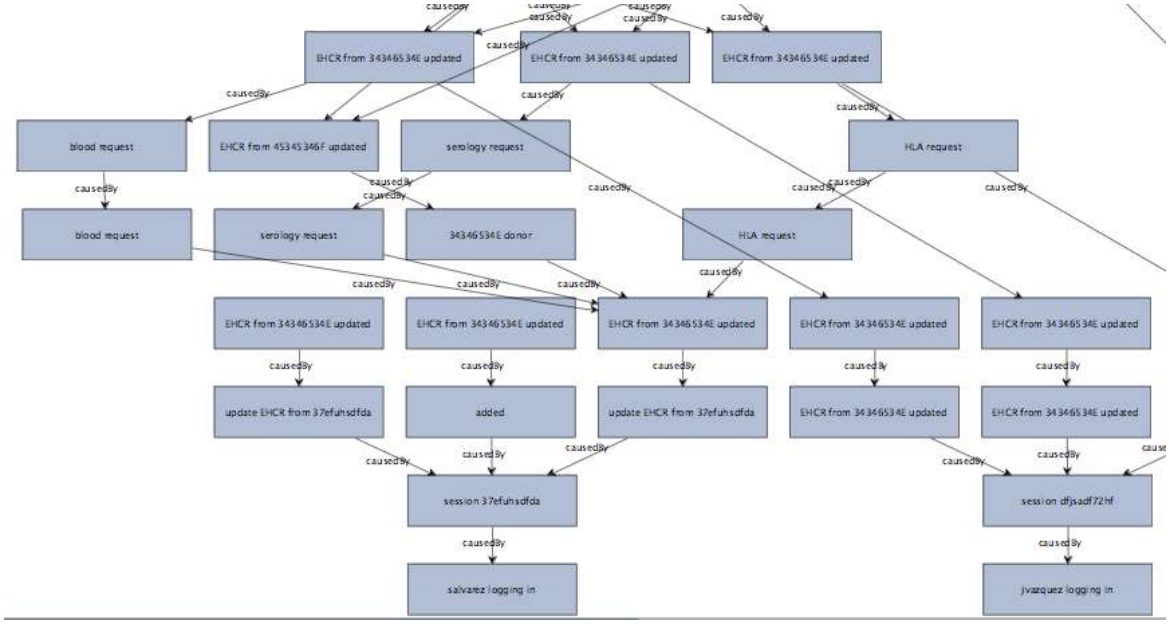
Q2.3: For a specific heart donation case, obtain the list of events related to it, with the list of times between each step, and the total time

- The user selects the donation cases list on the main menu of the web interface.
- The web interface retrieves the donation cases and shows them to the user.
- The user selects a donation case from the list.
- The web interface retrieves the record for that specific donation case and shows the record to the user.
- The user selects the option "Mark donation case for analysis" on the action toolbar.
- The web interface creates a copy of the tools Setup Protocol files, loading the queries for the donor and the provenance store location.
- The user selects "Event Analyzer" on the main menu.
- The tool portal is shown in the main frame.
- The user selects the Query portlet and chooses "Obtain events related to this case".
- The visualization tool is shown to the user.

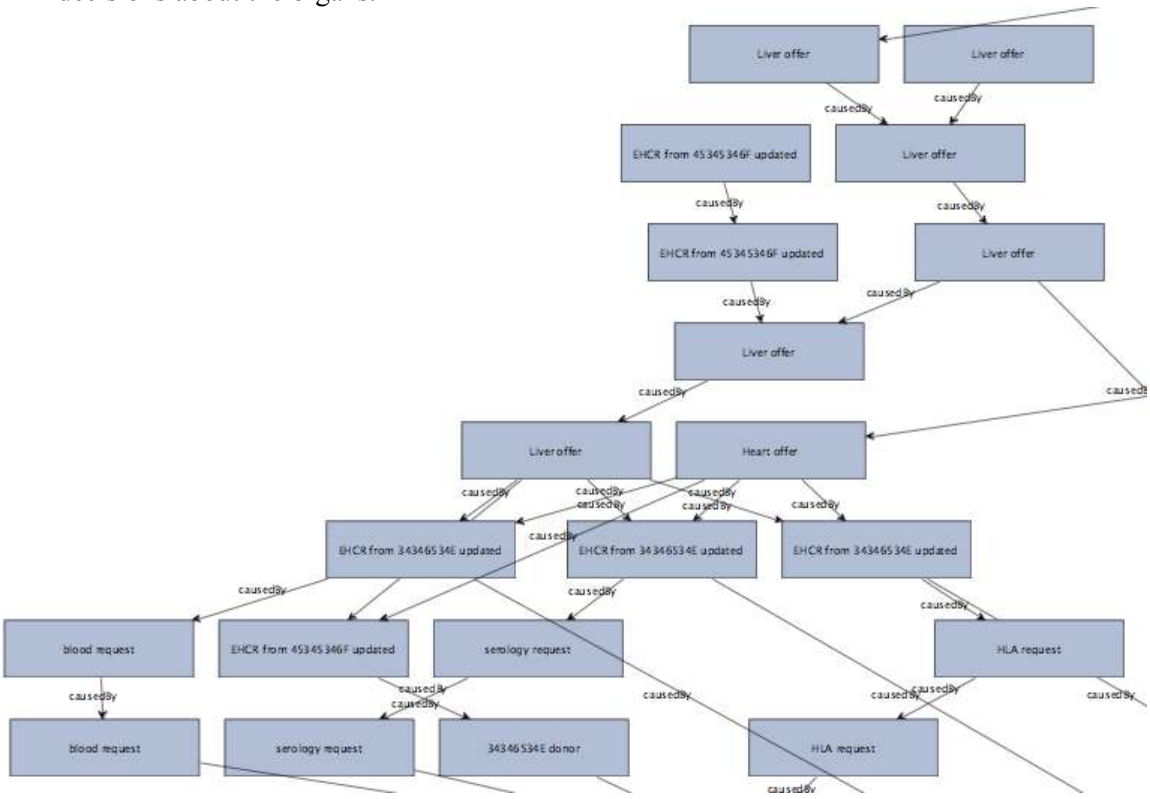


This query produces a graphical result. The whole process of the heart donation case is shown to the user, and we can identify four important parts of the diagram:

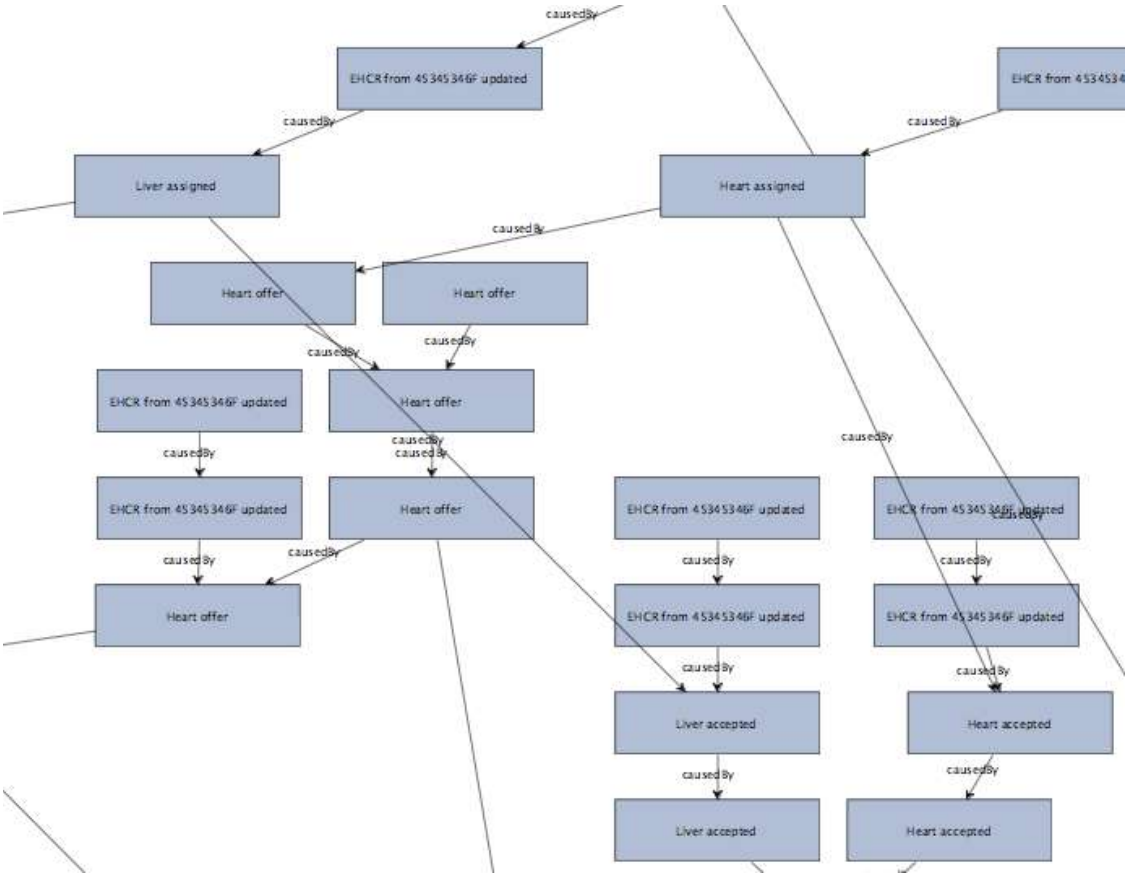
- Tests: in this part, the user can look at the test requests and results.



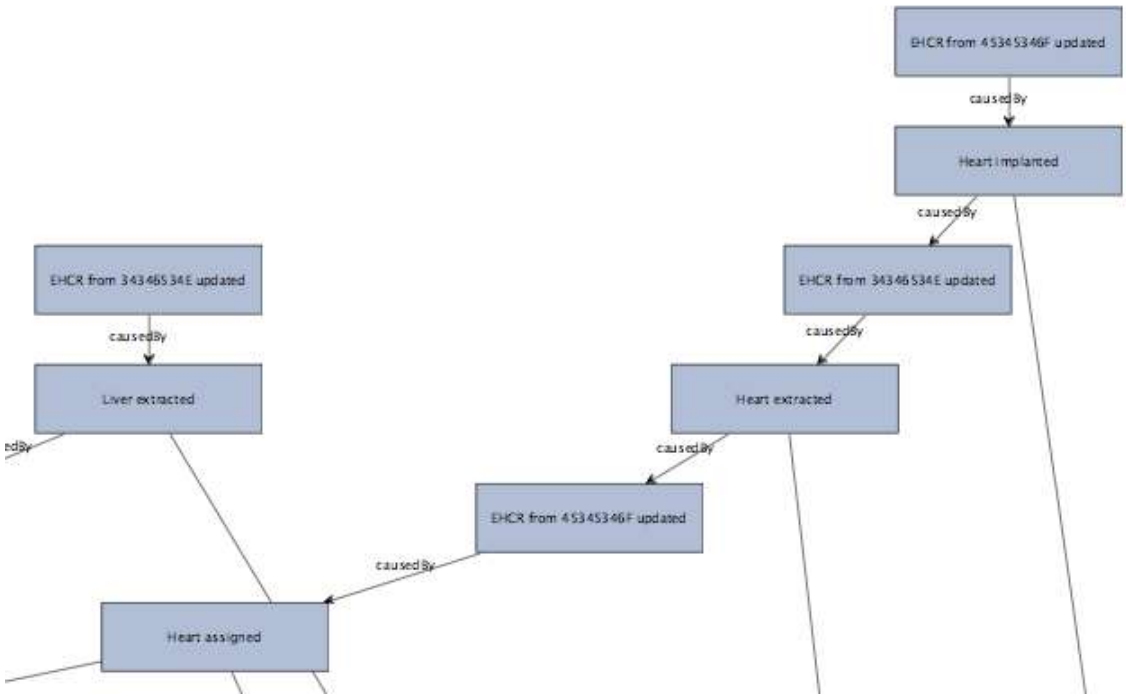
- Donor hospital decisions: these events represent Hospital A decisions. The arrows between these events and the ones in the Tests section represent that the tests are supporting the decisions about the organs.



- OTA and recipient hospital decisions: these events, triggered by the offer from Hospital A, represent the offer forwarding from OTA to the hospitals, and the acceptance or rejection of the hospitals being asked.



- Extraction and implant: these events are linked to another event of the previous section, the one that represents an hospital acceptance. The chain of events triggered are the representation of the extraction and the implant of the organ.



B.3 SCENARIO S3: A patient in hospital C that received a transplant becomes a donor for another transplant, accepted by first contacted hospital (hospital B)

This scenario will show how provenance traces of a previous transplant cases can be chained to get the full provenance of the current case.

B.3.1 Summary

Patient B2 from scenario S2 dies days after the liver implantation from causes that have nothing to do with the liver implantation; therefore, the team decides to declare Patient B2 as potential donor and offer the liver again for transplantation. No extra tests should be done and the liver offer is sent to OTA, which forwards it to the first hospital candidate (Hospital B) which rejects the offer again (because of the lack of reliable Biochemistry data). OTA forwards the offer to second hospital candidate (Hospital A) which accepts the offer. An extraction team from Hospital A travels to Hospital C and, after extraction and close examination of patient B2 organs, decides that the liver is in good condition to be implanted. Extraction team returns to Hospital A and then implants the organ to patient C1. Implantation fails (the liver is not performing well enough). The Hospital coordinator wants to know the provenance for this failure (solution: the Biochemistry data was not up-to-date, and the Biochemistry test from Lab A -which arrived too late and was not used in the decision) showed high levels of 2 substances that, if someone had noticed, could point out that the liver was already in no good condition).

B.3.2 PHASE A: the scenario run

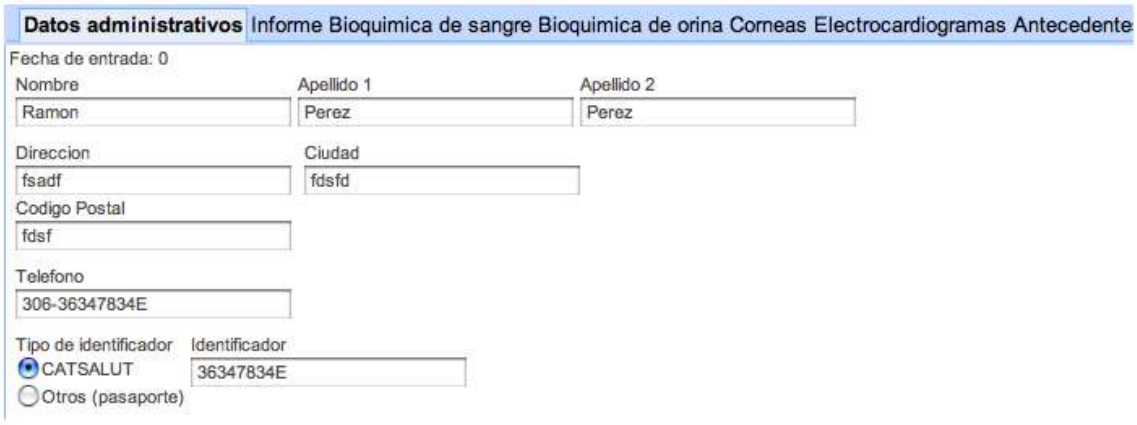
S3.1. Patient B2 in Hospital B declared as brain dead days after the implant. No information in the brain death declaration relates to the implant

- Doctor B in Hospital B opens the patient list of Hospital B in the web interface (see **Login**).
- The web interface shows Hospital B's patient list (*'Listado de pacientes'*) to Doctor B.

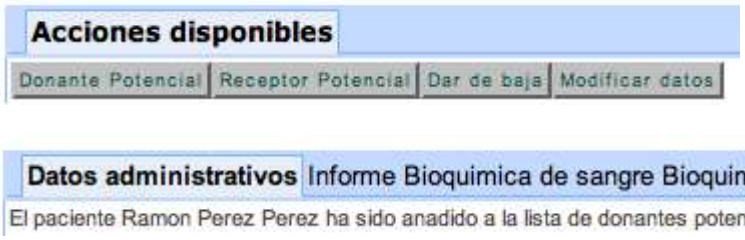
Listado de pacientes

Identificacion	Primer apellido	Segundo apellido	Nombre	Donante/Receptor	Fecha de entrada
36347834E	Perez	Perez	Ramon	Donante	0
34378433B	Garcia	Quinones	Carlos	Receptor	0
47347342F	Gomez	Ruiz	Laura	Donante	0
12345678A	Anderson		Mr.	Receptor	0

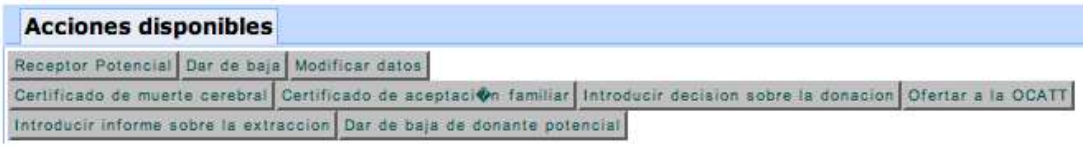
- Doctor B selects Patient B2 in the web interface.
- The web interface shows the full record of Patient B2 to Doctor B.



- Doctor B selects the "Declare Potential Donor" option (*'Donante Potencial'*) in the Patient B2 record screen. Then the system informs that the patient has been properly added to the Potential Donor List.

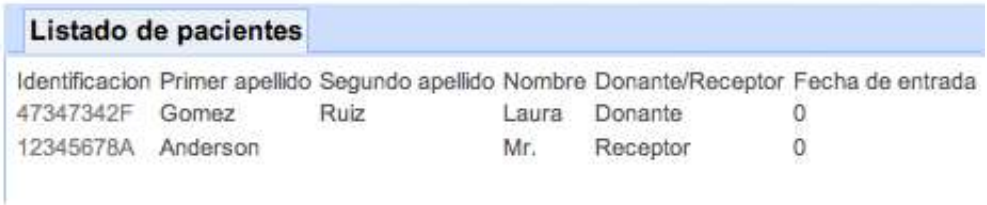


- Doctor B selects the "Declare Brain Death" option (*'Certificado de muerte cerebral'*) in the Patient B2 record screen.

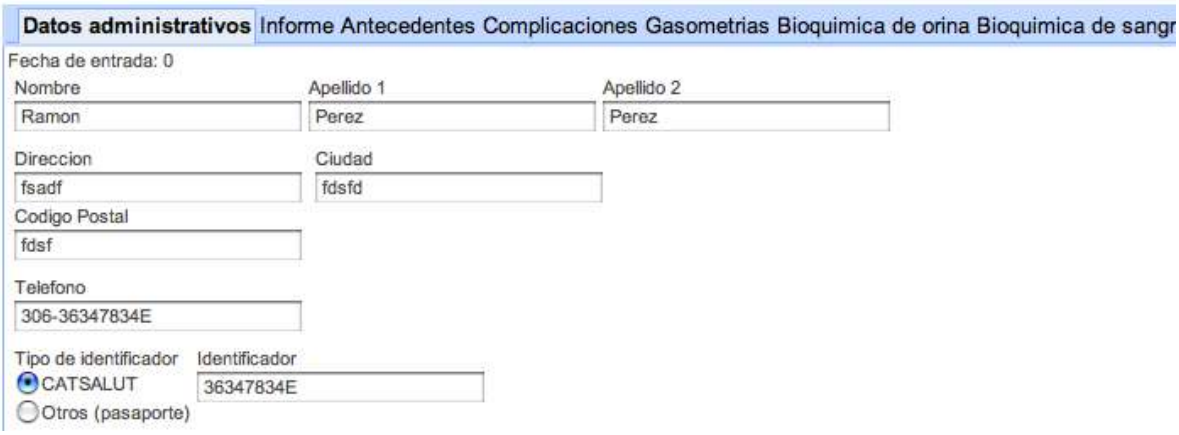


S3.2 Decision of donation done: patient B2's liver, supported by EHCR data and tests made before the implantation

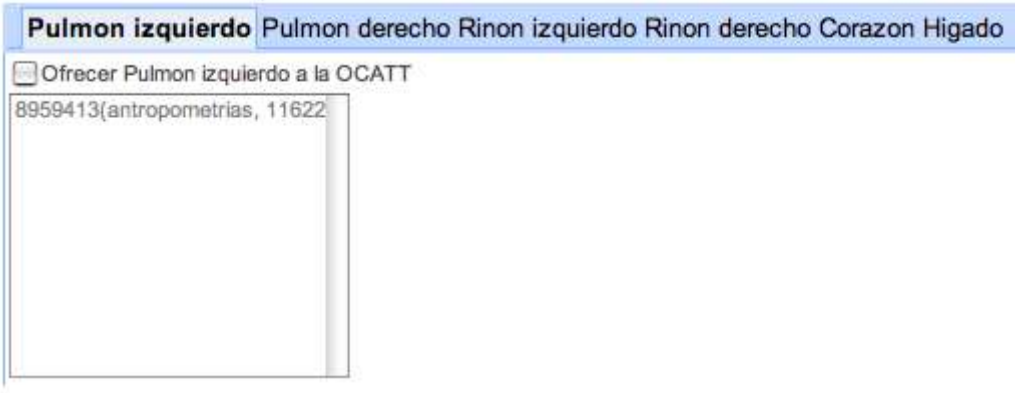
- Doctor B in Hospital B opens the patient list of Hospital B in the web interface.
- The web interface shows the patient list of Hospital B to Doctor B.



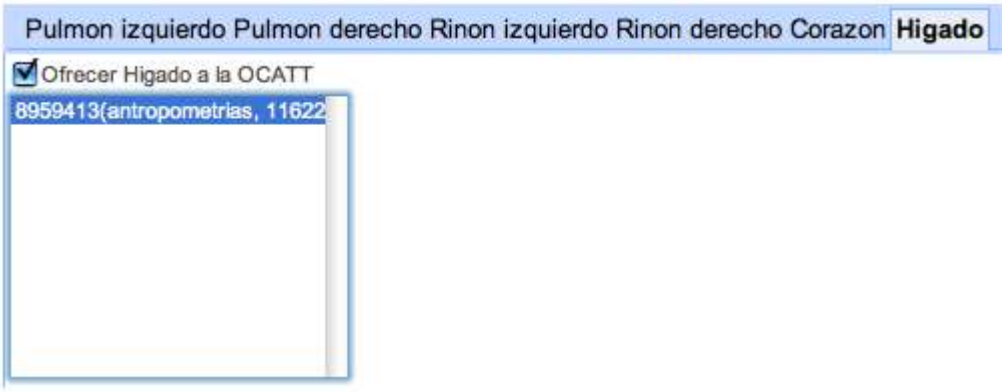
- Doctor B selects Patient B2 in the web interface. The web interface shows the full record of Patient B2 to Doctor B.



- Doctor B selects the "Give Donor Status" in the Patient B2 record screen.
- The web interface shows the list of organs to Doctor B.



- Doctor B selects liver in the web interface.
- The web interface shows the list of tests made for Patient B2, ordered by date.
- Doctor B selects the latest tests made before the implant.



S3.3. Message to OTA: Hospital A rejects liver offering

- A Doctor or a Management Staff Member in Hospital A reads the offer of a heart in the web interface and selects the "Decline Offer" option (*'Rechazar oferta'*).

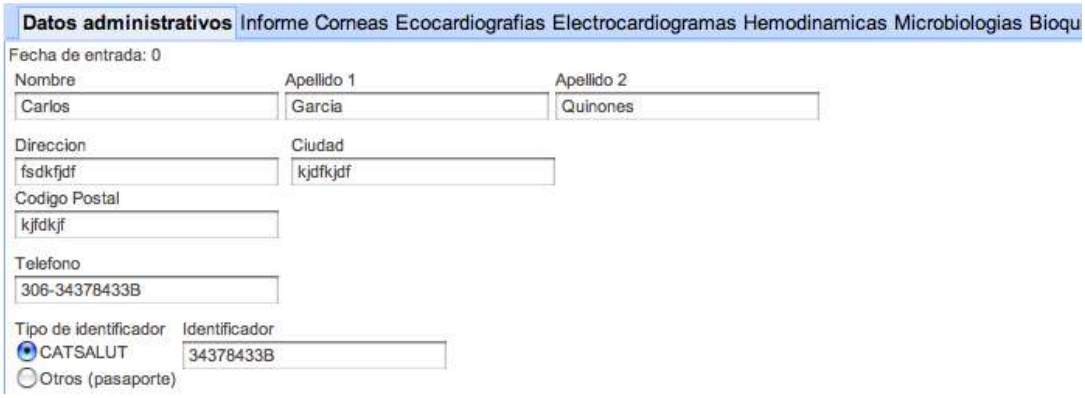
S3.4. Message to OTA: Hospital C accepts liver offering

- A Doctor or a Management Staff Member in Hospital C reads the offer of a heart in the web interface and selects the "Accept Offer" option(*'Aceptar oferta'*).

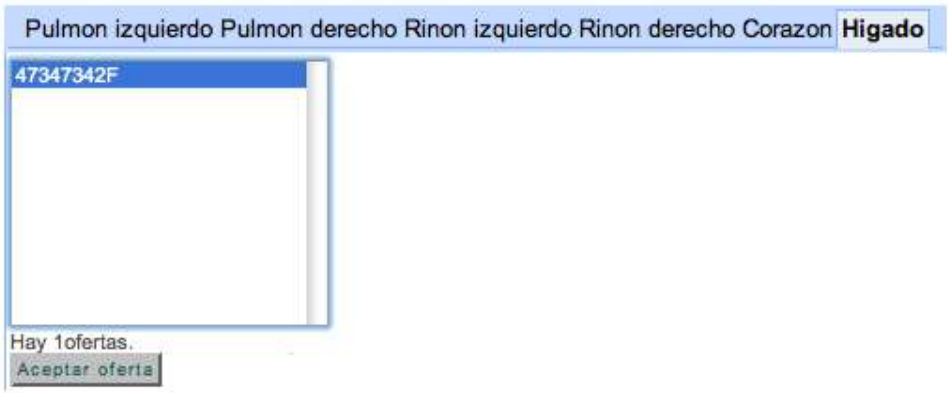
S3.5. Hospital C decides the recipient for the liver from Hospital C's liver waiting list: patient C1

- A Doctor or a Management Staff Member in Hospital C opens the waiting list of Hospital C in the web interface.
- The web interface shows the patient list, filtered by recipients, of Hospital C to the user who started the action.

- The same user selects Patient C1 in the web interface.
- The web interface shows the full record of Patient C1 to the user.



- The user selects the "Accept offer" button (*'Aceptar oferta'*) in the Patient C1 record screen



S3.6. Message to OTA + Extraction report by team from Hospital C: patient B2's liver accepted for donation

- Doctor C in Hospital B logs in the web interface.
- Doctor C in Hospital B opens the patient list of Hospital B in the web interface.
- The web interface shows the patient list of Hospital B to Doctor C.
- Doctor C selects Patient B2 in the web interface.
- The web interface shows the full record of Patient B2 to Doctor C.
- Doctor C selects the "Extraction Report" in the Patient B2 record screen.
- The web interface shows a list of the organs donated by Patient B2.
- Doctor C selects Liver from the list.
- The web interface shows a form for the Extraction Report to Doctor C.
- Doctor C fills the form, accepting the donation, in the web interface.

S3.7. Message to OTA + Implantation report by team from Hospital C: heart not implanted to patient C1

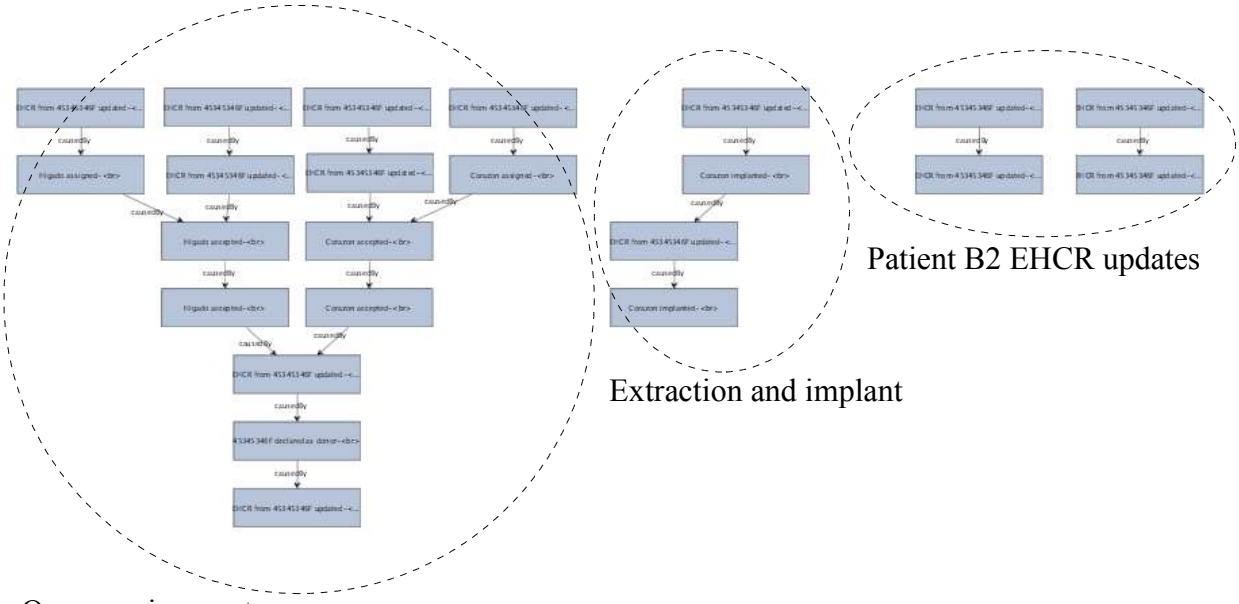
- Doctor C in Hospital C logs in the web interface.
- Doctor C in Hospital C opens the patient list of Hospital C in the web interface.
- The web interface shows the patient list of Hospital C to Doctor C.
- Doctor C selects Patient C1 in the web interface.
- The web interface shows the full record of Patient C1 to Doctor C.
- Doctor C selects the "Implant Report" in the Patient C1 record screen.
- The web interface shows a list of the organs being received by Patient C1.
- Doctor C selects Liver from the list.
- The web interface shows a form for the Implant Report to Doctor C.
- Doctor C fills the form in the web interface.

B.3.3 PHASE b: querying the Provenance stores

The queries will get not only the decisions taken in scenario S3, but also the decisions taken in scenario S2 (as the provenance for some decisions in scenario s3 comes from actions and data produced in scenario S2 related patient B1).

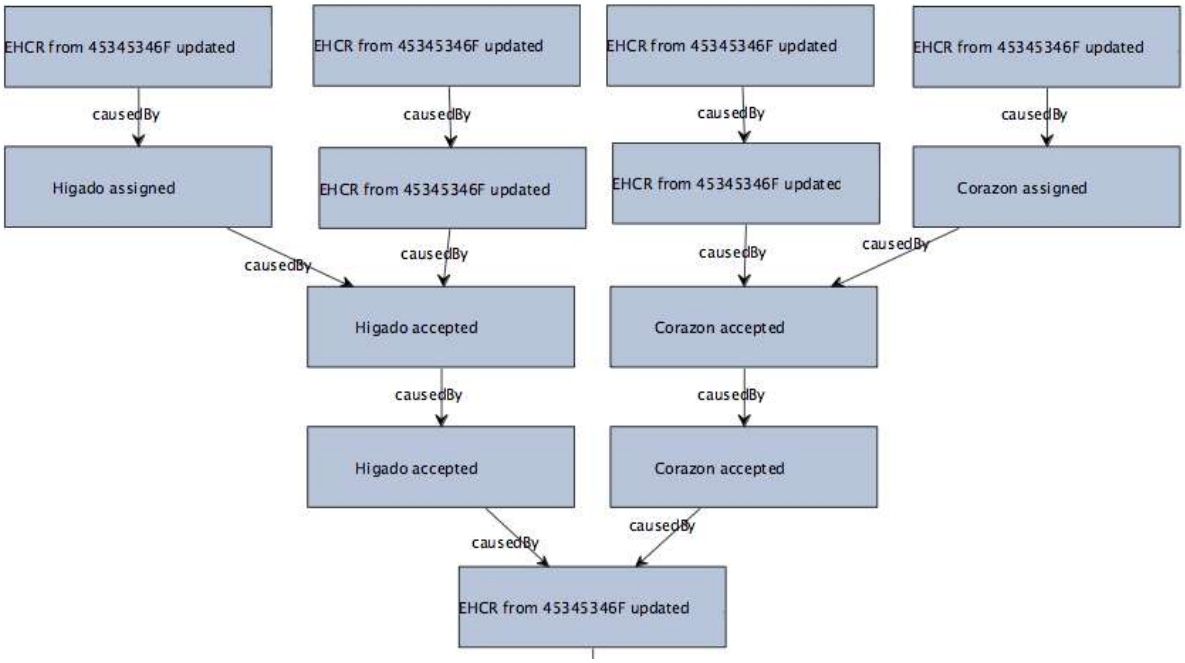
Q3.1: Obtain all events related to Patient B2

- The user selects the Patient B2 from the patient list, in the web interface.
- The web interface retrieves the data of Patient B2.
- The full record of Patient B2 is shown to the user.
- The user selects the option "Mark patient for analysis" on the action toolbar.
- The web interface creates a copy of the tools Setup Protocol files, loading the queries for a patient and the provenance store location.
- The user selects "Event Analyzer" on the main menu.
- The tool portal is shown in the main frame.
- The user selects the Query portlet and chooses "Obtain all events related to Patient B2".
- The visualization tool is shown to the user. In this case the user obtains the part of the workflow related directly with Patient B2.

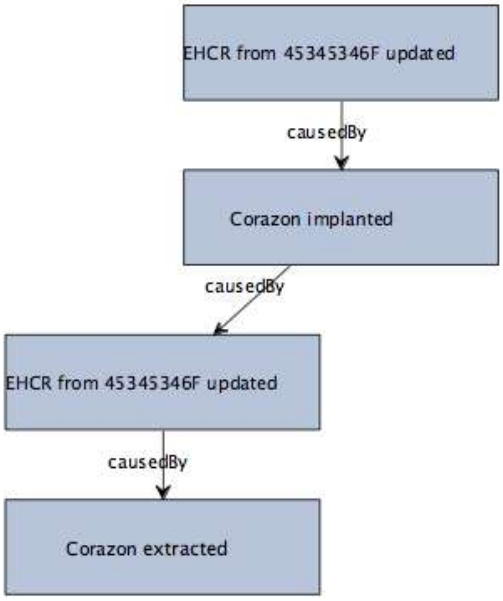


These are the events that the doctor will be able to see if this query is executed. In this case, the login procedures are not included in the query, so the diagram is clearer but less connected. The diagram can be divided in these parts:

- Organ assignment: the events drawn in this part of the diagram represent the assignment of the donor organ to the recipient. This is recorded from the recipient hospital.



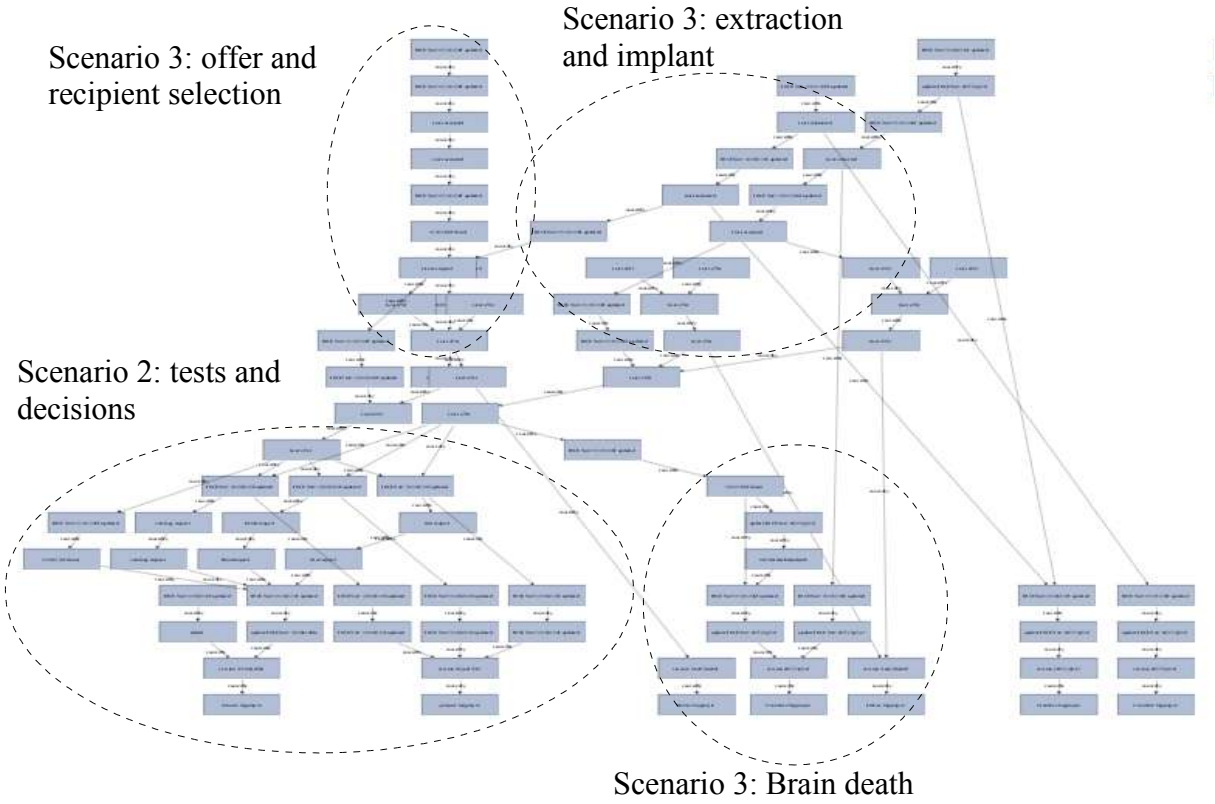
- Organ extraction and implant: these events represent the implantation of an organ to the recipient.



Q3.2: For a specific liver donation case, obtain the list of events related to it, with the list of times between each step, and the total time

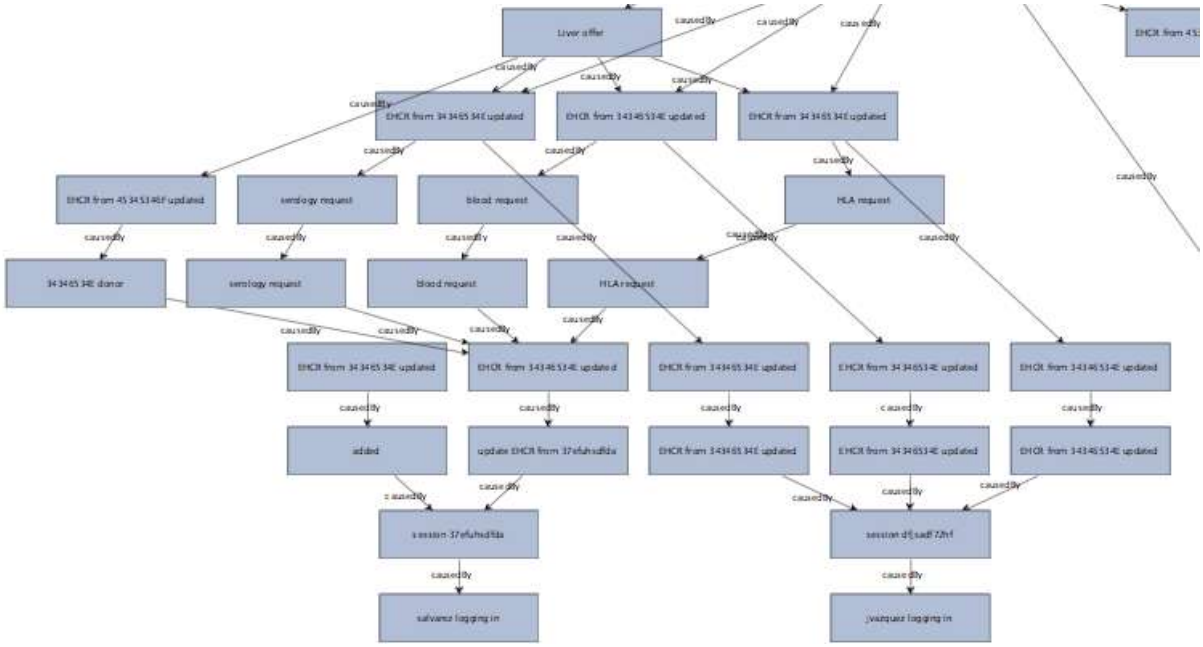
- The user selects the donation cases list on the main menu of the web interface.
- The web interface retrieves the donation cases and shows them to the user.
- The user selects a donation case from the list.

- The web interface retrieves the record for that specific donation case and shows the record to the user.
- The user selects the option "Mark donation case for analysis" on the action toolbar.
- The web interface creates a copy of the tools Setup Protocol files, loading the queries for the donor and the provenance store location.
- The user selects "Event Analyzer" on the main menu.
- The tool portal is shown in the main frame.
- The user selects the Query portlet and chooses "Obtain events related to this case".
- The visualization tool is shown to the user.

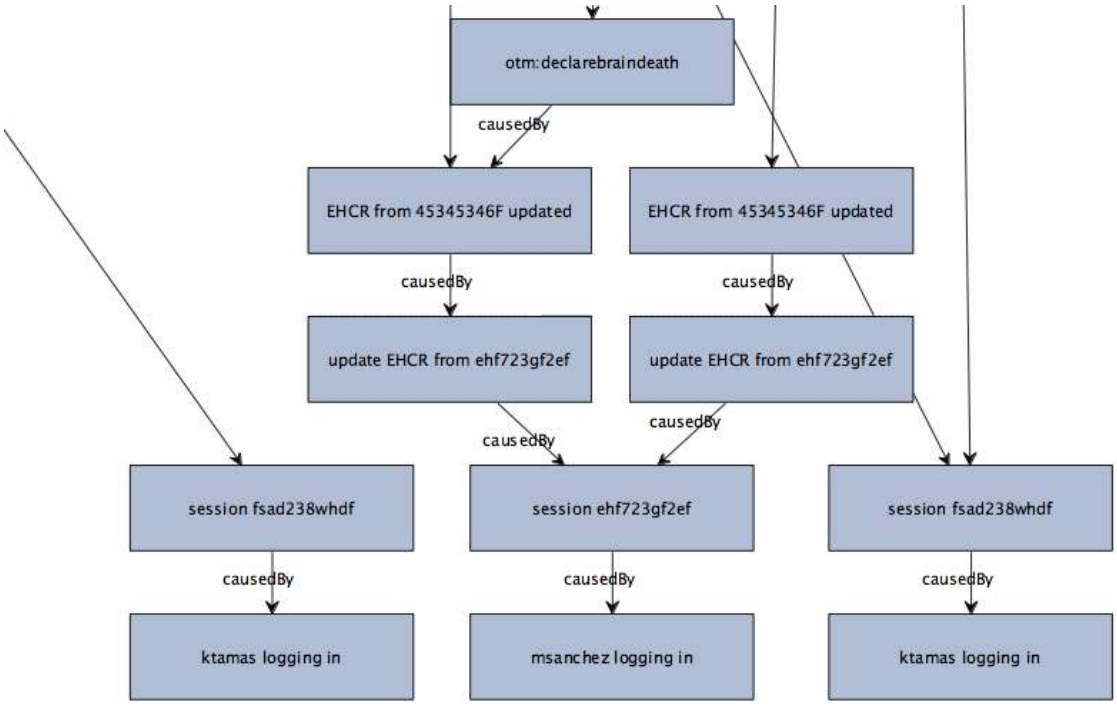


As the previous query, this one has a graphical result and includes events taking place in Scenario 2. The user can see the whole process of the liver donation case. Four main groups of events can be identified in the diagram:

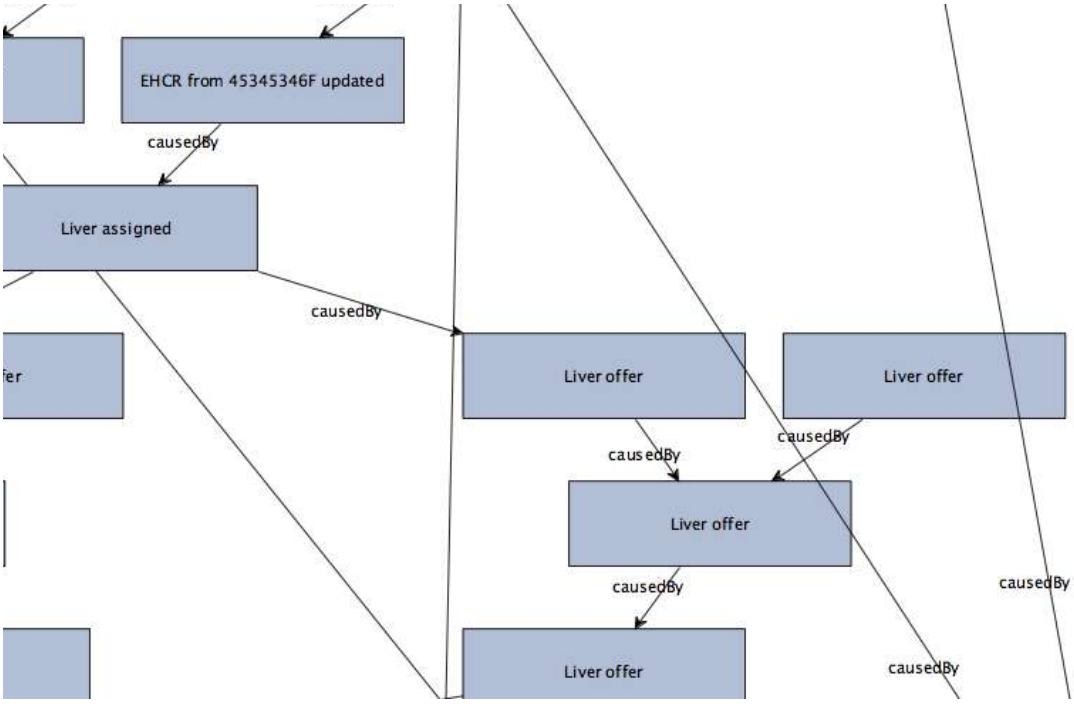
- Tests and decisions in Scenario 2: these are tests and decisions taken in the previous scenario that are related to the liver which will be re-transplanted.



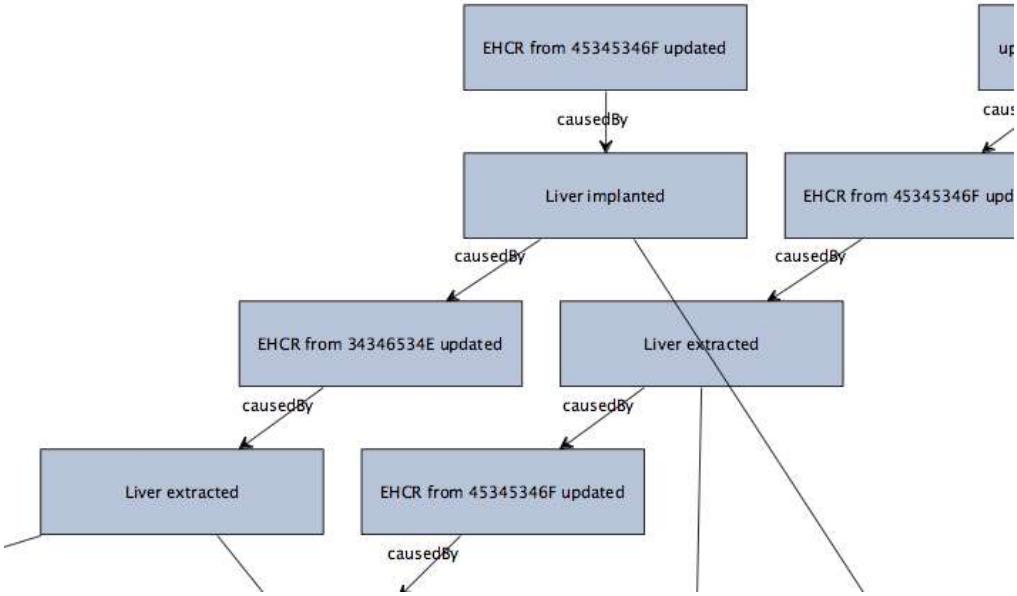
- Brain death report for the recipient in Scenario 2. The recipient in scenario 2 becomes donor in scenario 3.



- Organ offer and recipìent assignation: the graph shows the propagation of the Liver offer, the assignation of a recipient and that such assignation has an impact on the recipients' medical record.



- Extraction and implant in Scenario 3: The graphic also shows that the medical records of both patients are updated in the process.



References

[D2.1.1] Árpád Andics (ed.) **D2.1.1: User Requirements Document**. Technical report, MTA SZTAKI, February 2005. http://www.gridprovenance.org/deliverables/GRID_PROVENANCE-UserRequirements-D211-Month6.pdf

[D2.2.1] Árpád Andics (ed.). **D2.2.1: Software Requirements Document**. Technical report, MTA SZTAKI, February 2005. http://www.gridprovenance.org/deliverables/GRID_PROVENANCE-SoftwareRequirements-D221-Month6.pdf

[D3.1.1] Paul Groth, Sheng Jiang, Simon Miles, Steve Munroe, Victor Tan, Sofia Tsasakou, and Luc Moreau. **D3.1.1: An Architecture for Provenance Systems**. Technical report, University of Southampton, November 2006. http://eprints.ecs.soton.ac.uk/13216/

[D6.1.1] Omer F Rana. **D6.1.1: Tools Description Document**. Technical report, University of Cardiff, September 2005. http://www.gridprovenance.org/deliverables/GRID_PROVENANCE-ToolsSpec-D611-Month12.pdf

[D8.1.1] Javier Vázquez-Salceda, Steve Willmott, and Kifor Tamás and László Zs. Varga. **D8.1.1: Application 2: Organ Transplant Management. Specification of Mapping to Provenance Architecture, and Domain Specific Provenance Handling**. Technical report, UPC, September 2005. http://www.gridprovenance.org/deliverables/GRID_PROVENANCE-OTMSpec-D811-Month12.pdf

[D8.3.1] Javier Vázquez-Salceda, Sergio Álvarez, László Zs. Varga, and Kifor Tamás. **D8.3.1: Application 2: Final Deployment**. Technical report, UPC, November 2006. http://www.gridprovenance.org/deliverables/GRID_PROVENANCE-OTMDeployment-D821-Month27.pdf

[D9.3.3] John Ibbotson and Sheng Jiang. **D9.3.3: Final Functional Prototype**. Technical report, IBM United Kingdom, November 2006. http://www.gridprovenance.org/deliverables/GRID_PROVENANCE-FinalPrototype-D933-Month27.pdf

[D9.3.3a] Sheng Jiang, Luc Moreau, Paul Groth, Simon Miles, Steve Munroe, and Victor Tan. **D9.3.3a: Client Side Library Design and Implementation**. Technical report, University of Southampton, November 2006. http://www.gridprovenance.org/deliverables/GRID_PROVENANCE-ClientSideLibrary-D933a-Month27.pdf

[ENV13606] CEN/TC251 WG I.: Health Informatics-Electronic Healthcare Record Communication- Part 1-4, Final Draft prENV13606-1 (1999-2000).

[Miles 05] Simon Miles, Javier Vazquez. Project Internal document "Representing Provenance Data in the OTM application", July, 2005. http://twiki.gridprovenance.org/bin/viewauth/Restricted/OrganTransplantPStructure (project internal web site).

[RFC2141] R. Moats, "URN Syntax", Internet Engineering Task Force RFC 2141, May 1997. available online at http://www.ietf.org/rfc/rfc2141.txt .

[W3C05] D. Booth, H. Haas, F. McCabe et. al. "Web Services Architecture, W3C Working Group Note", 11 February 2004, available online at: http://www.w3.org/TR/2004/NOTE-ws-arch-20040211/ .