



# Security Requirements Document

## Sundhedsplatformen

phASE

Dec 31, 2025

This document has been generated by STS-Tool  
<http://www.sts-tool.eu>



## Table of Contents:

Introduction .....	1
Social and organizational models .....	2
Social View .....	3
<i>Social View Diagram</i> .....	3
<i>Stakeholders</i> .....	4
<i>Stakeholders' documents</i> .....	4
<i>Stakeholders' documents and goals</i> .....	7
<i>Goal Refinement</i> .....	11
<i>Goal Contributions</i> .....	14
<i>Stakeholders Interactions</i> .....	14
Goal Delegations .....	14
Document Transmission .....	19
<i>Organisational Constraints</i> .....	25
Events.....	26
Information View .....	27
<i>Information View Diagram</i> .....	27
<i>Modelling Ownership</i> .....	28
<i>Representation of Information</i> .....	29
<i>Structure of Information and Documents</i> .....	30
Authorization View .....	32
<i>Authorization View Diagram</i> .....	32
<i>Authorization Flow</i> .....	33
Security Requirements.....	36
Well-formedness Analysis.....	118
Security Analysis .....	119
Appendix A.....	120
Appendix B .....	123
Appendix C .....	125



## Introduction

This document describes the security requirements for the "Sundhedsplatformen" project. It provides a detailed description of: (I)social and organizational model, while capturing security requirements and automated analysis results;

## Social and organizational models

This section provides a detailed description of the socio-technical security requirements models from different views (*Social, Information, Authorization*) and then presents the list of *security requirements* derived from them.

The *Social view* represents stakeholders as intentional and social entities, representing their goals and important information in terms of documents, together with their interactions with other actors to achieve these goals and to exchange information. Stakeholders express constraints over their interactions in terms of *security needs*. The *Information view* represents the informational content of stakeholders' documents, showing how information and documents are interconnected, as well as how they are composed respectively. The *Authorization view* represents which stakeholders own what information, and captures the flow of permissions or prohibitions from one stakeholder to another. The modelling of authorizations expresses other *security needs* related to the way information is to be manipulated.

The section ends with the list of *security requirements* for the system to be expressed in terms of *social commitments*, namely promises with contractual validity stakeholders make to one another. The security requirements are derived automatically once the modelling is done and the designer has captured the security needs expressed by stakeholders. Whenever a security need is expressed over an interaction from one stakeholder to the other, a commitment on the opposite direction is expected from the second stakeholder to satisfy the security need.

## Social View

The social view shows the involved stakeholders, which are represented as *roles* and *agents*. Agents refer to actual participants (stakeholders) known when modelling the Sundhedsplatformen project, whereas roles are a generalisation (abstraction) of agents. To capture the connection between roles and agents, the *play* relation is used to express the fact that certain agents play certain roles.

Stakeholders have goals to achieve and they make use of different information to achieve these goals. They interact with one another mainly by *delegating goals* and *exchanging information*. Information is represented by means of documents, which actors manipulate to achieve their goals.

### Social View Diagram

Figure 1 presents the graphical representation of the social view (a larger picture is shown in appendix A).

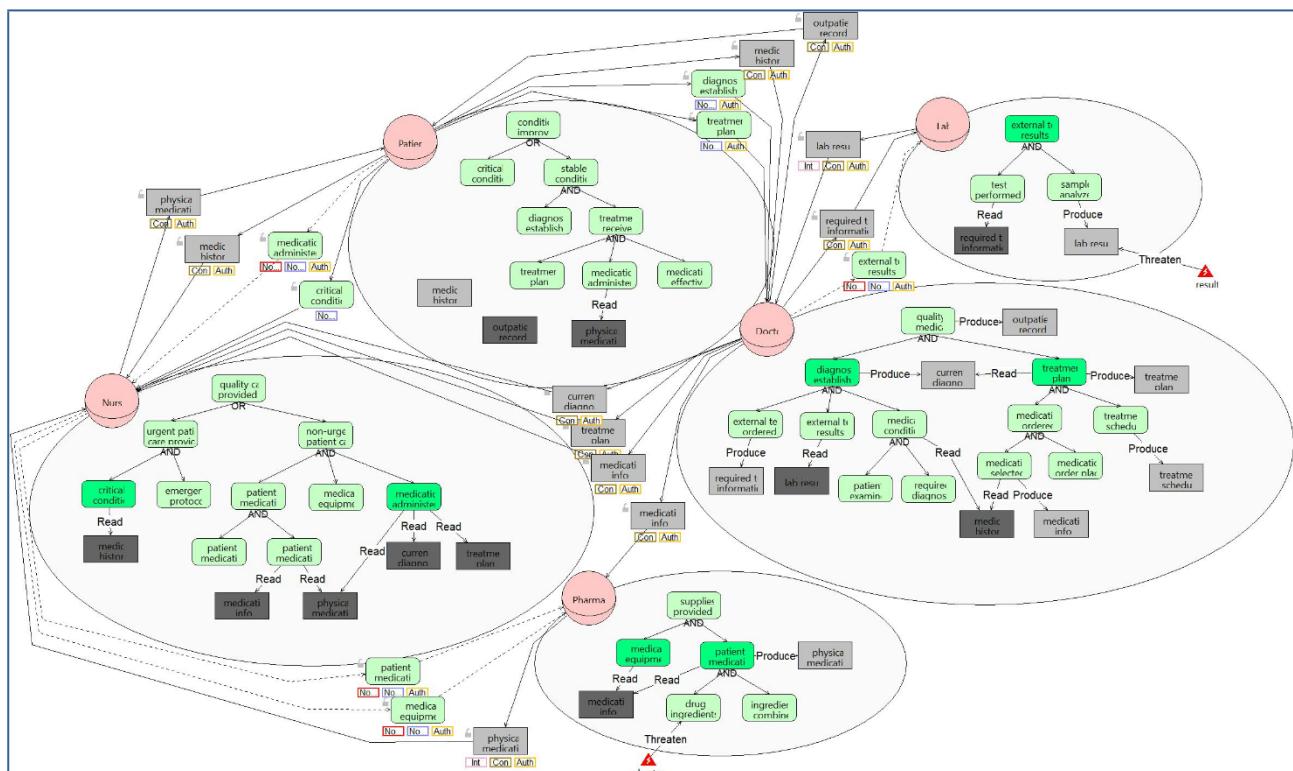


Figure 1 - Social View for the Sundhedsplatformen project

## Stakeholders

This section describes the stakeholders identified in the Sundhedsplatformen project. Stakeholders are represented as roles or agents.

In particular, identified roles are: *Patient*, *Doctor*, *Lab*, *Nurse* and *Pharmacy* (Figure 1). Table 1 summarise the stakeholders.

Role	Description	Mission	Purpose
Patient			
Doctor			
Lab			
Nurse			
Pharmacy			

Table 1 - Roles in the Sundhedsplatformen project.

In the Sundhedsplatformen project there are no plays relationships taking place for the given agents/roles.

## Stakeholders' documents

Stakeholders have documents they possess or exchange with others to achieve their goals. Documents are represented within the rationale of the role/agent (Figure 1).

In the Sundhedsplatformen project (Figure 1) we have:

- **Patient** has document *medical history*. Moreover it has document *outpatient record* provided by *Doctor* and document *physical medication* provided by *Nurse*.
- **Doctor** has documents *outpatient record*, *treatment plan*, *medication info*, *required test information*, *current diagnosis* and *treatment schedule*. Moreover it has document *medical history* provided by *Patient* and document *lab results* provided by *Lab*.
- **Lab** has document *lab results*. Moreover it has document *required test information* provided by *Doctor*.
- **Nurse** has document *treatment plan* provided by *Doctor*, document *medical history* provided by *Patient*, document *medication info* provided by *Doctor*, document *current diagnosis* provided by *Doctor* and document *physical medication* provided by *Pharmacy*.
- **Pharmacy** has document *physical medication*. Moreover it has document *medication info* provided by *Doctor*.

Table 2 summarises stakeholders' documents for the Sundhedsplatformen project.

Agent/Role	Document	Description
Patient	outpatient record	
	physical medication	
	medical history	

	lab results
	outpatient record
	treatment plan
	medication info
Doctor	required test information
	current diagnosis
	treatment schedule
	medical history
Lab	lab results
	required test information
	physical medication
	treatment plan
Nurse	current diagnosis
	medical history
	medication info
Pharmacy	physical medication
	medication info

Table 2 - Stakeholders' documents in the Sundhedsplatformen project

### Stakeholders' documents and goals

Stakeholders' documents are linked to their goals: they read (make) documents to achieve their goals, they modify documents while achieving their goals, and they may produce documents from achieving their goals.

In the Sundhedsplatformen project (Figure 1) stakeholders' documents and goals are related as follows:

- **Patient** reads document *physical medication* to achieve goal *medication administered*.
- **Doctor** produces document *required test information* to achieve goal *external tests ordered*, reads document *lab results* to achieve goal *external test results available*, produces document *treatment schedule* to achieve goal *treatment schedule planned*, produces document *current diagnosis* to achieve goal *diagnosis established*, reads document *medical history* and produces document *medication info* to achieve goal *medication selected*, reads document *current diagnosis* and produces document *treatment plan* to achieve goal *treatment plan established*, produces document *outpatient record* to achieve goal *quality medical expertise provided* and reads document *medical history* to achieve goal *medical condition assessed*.
- **Lab** reads document *required test information* to achieve goal *test performed on patient* and produces document *lab results* to achieve goal *samples analyzed*.
- **Nurse** reads document *treatment plan*, reads document *physical medication* and reads document *current diagnosis* to achieve goal *medication administered*, reads document *medical history* to

achieve goal *critical condition stabilized* and *reads document medication info* and *reads document physical medication* to achieve goal *patient medication verified*.

- **Pharmacy** *reads document medication info* and *produces document physical medication* to achieve goal *patient medication prepared* and *reads document medication info* to achieve goal *medical equipment provided*.

Table 3 summarises goal-document relations for all stakeholders in the Sundhedsplatformen project.

<b>Agent/Role</b>	<b>Goal</b>	<b>Document</b>	<b>Relation</b>
Patient	medication administered	physical medication	Read
	external tests ordered	required test information	Produce
	external test results available	lab results	Read
	treatment schedule planned	treatment schedule	Produce
	diagnosis established	current diagnosis	Produce
	medication selected	medical history	Read
		medication info	Produce
		current diagnosis	Read
		treatment plan	Produce
	quality medical expertise provided	outpatient record	Produce
Doctor	medical condition assessed	medical history	Read
	test performed on patient	required test information	Read
	samples analyzed	lab results	Produce
		treatment plan	Read
Lab	medication administered	physical medication	Read
		current diagnosis	Read
	critical condition stabilized	medical history	Read
	patient medication verified	medication info	Read
		physical medication	Read
Nurse	patient medication prepared	medication info	Read
		physical medication	Produce
	medical equipment provided	medication info	Read
Pharmacy			

Table 3 - Relation of stakeholders' documents to their goals

## Goal Refinement

Stakeholders have goals to achieve. Goals are represented within the rationale (round compartment attached to the role/agent, see Figure 1) of the role/agent representing the stakeholder. They achieve their goals by further refining them into finer-grained goals (subgoals) by means of AND/OR-decompositions. AND-decompositions structurally refine a goal into multiple subgoals (all AND subgoals need to be achieved for the goal to be achieved), while OR-decompositions represent alternative ways for achieving a goal (at least one of the subgoals in the OR-decomposition needs to be achieved for the goal to be achieved).

In the Sundhedsplatformen project (Figure 1) we have:

- **Patient** has to achieve goal *condition improved*. To achieve *treatment received*, Patient should achieve goal *medication administered*, goal *medication effective* and goal *treatment plan established*. To achieve *stable condition improved*, Patient should achieve goal *diagnosis established* and goal *treatment received*. To achieve *condition improved*, Patient should achieve either goal *stable condition improved* or goal *critical condition stabilized*.
- **Doctor** has to achieve goal *quality medical expertise provided*. To achieve *diagnosis established*, Doctor should achieve goal *external test results available*, goal *medical condition assessed* and goal *external tests ordered*. To achieve *medical condition assessed*, Doctor should achieve goal *required diagnostic tests performed* and goal *patient examined*. To achieve *quality medical expertise provided*, Doctor should achieve goal *diagnosis established* and goal *treatment plan established*. To achieve *treatment plan established*, Doctor should achieve goal *treatment schedule planned* and goal *medication ordered*. To achieve *medication ordered*, Doctor should achieve goal *medication selected* and goal *medication order placed*.
- **Lab** has to achieve goal *external test results available*. To achieve *external test results available*, Lab should achieve goal *test performed on patient* and goal *samples analyzed*.
- **Nurse** has to achieve goal *quality care provided for patients*. To achieve *patient medication available*, Nurse should achieve goal *patient medication verified* and goal *patient medication prepared*. To achieve *quality care provided for patients*, Nurse should achieve either goal *urgent patient care provided* or goal *non-urgent patient care provided*. To achieve *urgent patient care provided*, Nurse should achieve goal *critical condition stabilized* and goal *emergency protocol initiated*. To achieve *non-urgent patient care provided*, Nurse should achieve goal *patient medication available*, goal *medical equipment provided* and goal *medication administered*.
- **Pharmacy** has to achieve goal *supplies provided for hospitals*. To achieve *supplies provided for hospitals*, Pharmacy should achieve goal *patient medication prepared* and goal *medical equipment provided*. To achieve *patient medication prepared*, Pharmacy should achieve goal *drug ingredients in stock* and goal *ingredients combined*.

Table 4 summarises the goals of each agent/role in the Sundhedsplatformen project and how they are decomposed, when applicable.

Agent/Role	Goal	Dec. Type	Subgoals
Patient	condition improved	OR	stable condition improved critical condition stabilized

Doctor	quality medical expertise provided	AND	diagnosis established treatment plan established
Lab	external test results available	AND	test performed on patient samples analyzed
Nurse	quality care provided for patients	OR	urgent patient care provided non-urgent patient care provided
Pharmacy	supplies provided for hospitals	AND	patient medication prepared medical equipment provided

Table 4 - Goal Decompositions

### Goal Contributions

Goals can contribute one to another. A contribution identifies the impact the fulfilment of one goal has on the fulfilment of another goal. This impact can be either positive or negative, and is represented with "++" and "--" respectively. Positive contribution means that the achievement of a goal also achieves the other goal. Negative contribution means that the achievement of a goal inhibits the achievement of another goal.

In the Sundhedsplatformen project there are no contribution relations taking place for the given agents/roles.

### Stakeholders Interactions

This section describes stakeholders' interactions, providing insights on whom they interact with to fulfil their desired objectives, as well as which are the stakeholders that rely on them to fulfil their respective goals. This kind of interaction is carried out by means of *goal delegations*.

To achieve their goals stakeholders might need specific information. If they do not possess this information, they may ask other stakeholders to provide them documents. *Document transmission* is used to capture this interaction.

### Goal Delegations

Stakeholders interact with others to achieve some of their goals by means of goal delegations. Goal delegations are graphically represented as a relation that starts from a delegator actor to a delegatee actor (following the direction of the arrow), having a rounded corner rectangle representing the goal being delegated. Security needs are graphically specified as labels that appear below the delegated goal (Figure 1).

The following description enlists all the delegations from one role/agent to the others. When applicable, security needs expressed over the delegations are enumerated.

In the Sundhedsplatformen project (Figure 1), we have the following goal delegations:

- **Patient** delegates goal *diagnosis established* to **Doctor**.

The following security needs apply to this delegation:

Non Repudiation: acceptance and Authentication: delegator.

- **Patient** delegates goal *medication administered* to **Nurse**.

The following security needs apply to this delegation:

No-Delegation, Non Repudiation: acceptance and Authentication: delegator.

- **Patient** delegates goal *treatment plan established* to **Doctor**.

The following security needs apply to this delegation:

Non Repudiation: acceptance and Authentication: delegator.

- **Patient** delegates goal *critical condition stabilized* to **Nurse**.

The following security needs apply to this delegation:

Non Repudiation: acceptance.

- **Doctor** delegates goal *external test results available* to **Lab**.

The following security needs apply to this delegation:

No-Delegation, Non Repudiation: delegation-acceptance and Authentication: delegatee.

- **Nurse** delegates goal *patient medication prepared* to **Pharmacy**.

The following security needs apply to this delegation:

No-Delegation, Non Repudiation: delegation-acceptance and Authentication: delegatee.

- **Nurse** delegates goal *medical equipment provided* to **Pharmacy**.

The following security needs apply to this delegation:

No-Delegation, Non Repudiation: delegation-acceptance and Authentication: delegatee.

Table 5 summarises *goal delegations*, together with the eventual *security needs* when applicable, and eventual description respectively.

<b>Delegator</b>	<b>Goal</b>	<b>Delegatee</b>	<b>Security Needs</b>	<b>Delegation Description</b>
Patient	diagnosis established	Doctor	<b>Non Repudiation:</b> <i>acceptance</i> <b>Authentication:</b> <i>delegator</i>	
	medication administered	Nurse	<b>No-Delegation</b> <b>Non Repudiation:</b> <i>acceptance</i> <b>Authentication:</b> <i>delegator</i>	
	treatment plan established	Doctor	<b>Non Repudiation:</b> <i>acceptance</i> <b>Authentication:</b> <i>delegator</i>	
	critical condition stabilized	Nurse	<b>Non Repudiation:</b> <i>acceptance</i>	
Doctor	external test results	Lab	<b>No-Delegation</b>	

	available		<b>Non Repudiation:</b> <i>delegation-acceptance</i> <b>Authentication:</b> <i>delegatee</i>
Nurse	patient medication prepared	Pharmacy	<b>No-Delegation</b> <b>Non Repudiation:</b> <i>delegation-acceptance</i> <b>Authentication:</b> <i>delegatee</i>
	medical equipment provided	Pharmacy	<b>No-Delegation</b> <b>Non Repudiation:</b> <i>delegation-acceptance</i> <b>Authentication:</b> <i>delegatee</i>

Table 5 - Goal Delegations and Security Needs

### Document Transmission

Stakeholders exchange information by means of documents with other stakeholders. The following description enlists all the transmission from one role/agent representing the stakeholder, to other roles/agents. *Document transmission* is represented as an arrow from the transmitter to the receiver, with a rectangle representing the document. The security needs expressed over the transmission are described, if applicable. Security needs are specified with the help of labels that appear below the document being transmitted.

In the Sundhedsplatformen project (Figure 1), we have the following *document transmissions*:

- **Patient** transmit document *medical history* to **Doctor**.  
The following security needs apply to this transmission:  
Confidentiality: receiver and Authentication: receiver.
- **Patient** transmit document *medical history* to **Nurse**.  
The following security needs apply to this transmission:  
Confidentiality: receiver and Authentication: receiver.
- **Doctor** transmit document *outpatient record* to **Patient**.  
The following security needs apply to this transmission:  
Confidentiality: sender and Authentication: receiver.
- **Doctor** transmit document *required test information* to **Lab**.  
The following security needs apply to this transmission:  
Confidentiality: system and Authentication: receiver.
- **Doctor** transmit document *treatment plan* to **Nurse**.  
The following security needs apply to this transmission:  
Confidentiality: system and Authentication: receiver.
- **Doctor** transmit document *current diagnosis* to **Nurse**.  
The following security needs apply to this transmission:

Confidentiality: system and Authentication: receiver.

- **Doctor** transmit document *medication info* to **Pharmacy**.

The following security needs apply to this transmission:

Confidentiality: system and Authentication: receiver.

- **Doctor** transmit document *medication info* to **Nurse**.

The following security needs apply to this transmission:

Confidentiality: system and Authentication: receiver.

- **Lab** transmit document *lab results* to **Doctor**.

The following security needs apply to this transmission:

Integrity: system, Confidentiality: system and Authentication: receiver.

- **Nurse** transmit document *physical medication* to **Patient**.

The following security needs apply to this transmission:

Confidentiality: sender and Authentication: receiver.

- **Pharmacy** transmit document *physical medication* to **Nurse**.

The following security needs apply to this transmission:

Integrity: system, Confidentiality: system and Authentication: receiver.

Table 6 summarises the *document transmissions* for the Sundhedsplatformen project.

Transmitter	Document	Receiver	Security Needs	Transmission Descr.
Patient	medical history	Doctor	Confidentiality: receiver Authentication: receiver	
	medical history	Nurse	Confidentiality: receiver Authentication: receiver	
	outpatient record	Patient	Confidentiality: sender Authentication: receiver	
	required test information	Lab	Confidentiality: system Authentication: receiver	
Doctor	treatment plan	Nurse	Confidentiality: system Authentication: receiver	
	current diagnosis	Nurse	Confidentiality: system Authentication: receiver	
	medication info	Pharmacy	Confidentiality:	

			<b>Authentication:</b> <i>system receiver</i>
	medication info	Nurse	<b>Confidentiality:</b> <i>system</i> <b>Authentication:</b> <i>receiver</i>
Lab	lab results	Doctor	<b>Integrity:</b> <i>system</i> <b>Confidentiality:</b> <i>system</i> <b>Authentication:</b> <i>receiver</i>
Nurse	physical medication	Patient	<b>Confidentiality:</b> <i>sender</i> <b>Authentication:</b> <i>receiver</i>
Pharmacy	physical medication	Nurse	<b>Integrity:</b> <i>system</i> <b>Confidentiality:</b> <i>system</i> <b>Authentication:</b> <i>receiver</i>

Table 6 - Document Transmissions and Security Needs

## Organisational Constraints

Apart from the security needs actors specify over their interactions, there are others, which are dictated either by the organisation, business rules and regulations, or law. In this section we enlist these constraints, together with the security requirements derived from them. Currently, the language supports these organisational constraints: *Separation of Duties (SoD)* and *Binding of Duties (BoD)*. Graphically we represent these constraints using a similar notation to that used in workflows, as a circle with the *unequal* sign within and as a circle with the *equals* sign within, respectively. The relations are symmetric, and as such they do not have any arrows pointed to the concepts they relate (being these roles or goals).

In the Sundhedsplatformen project there are no organisational constraints specified.

## Events

Table 7 represents all the events modeled in the project Sundhedsplatformen together with the set of elements each event threatens. Additionally, for each reported event a textual description is provided.

Event name	Threatened elements	Description
shortage	Goal: drug ingredients in stock	
result mistake	Document: lab results	

Table 7 - Events

## Information View

The information view gives a structured representation of the information and documents in the Sundhedsplatformen project. It shows what is the informational content of the documents represented in the social view. Information is represented by one or more documents (*tangible by*), and the same document can make tangible multiple information entities. Moreover, the information view considers composite documents (information) capturing these by means of *part of* relations.

### Information View Diagram

Figure 2 presents the graphical representation of the information view (a larger picture is shown in appendix A).

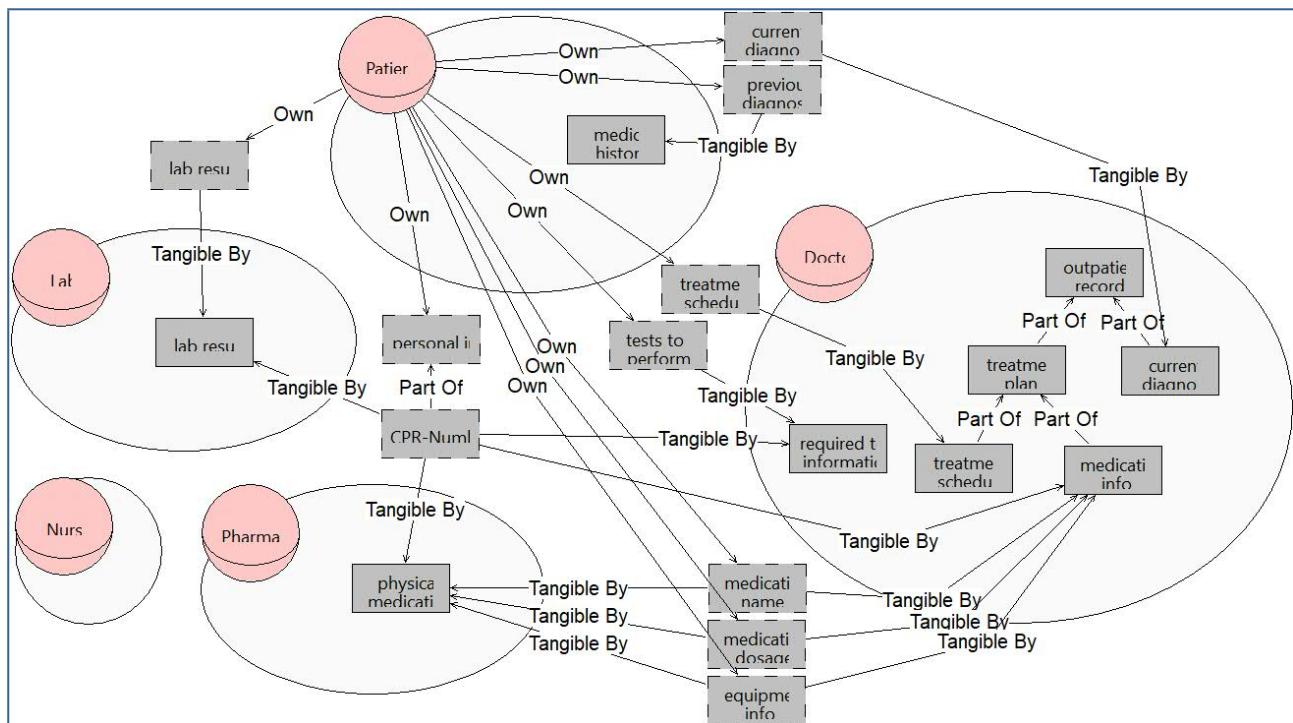


Figure 2 - Information View for the Sundhedsplatformen project

## Modelling Ownership

The information view represents also who are the *owners* of the information that is being manipulated through the documents that represent them in the social view.

The owners for the different information in the Sundhedsplatformen project are summarised in Table 8.

Agent/Role	Information	Description
Patient	previous diagnoses	
	personal info	
	treatment schedule	
	lab results	
	current diagnosis	
	tests to be performed	
	medication name	
	medication dosage	
	equipment info	

Table 8 - Information owners

## Representation of Information

Information is represented (*made tangible by*) by documents, which stakeholders have and exchange.

The documents stakeholders in the Sundhedsplatformen project (Figure 2) have and exchange with one another contain the information as summarised in Table 9:

Information	Document	Description
treatment schedule	treatment schedule	
current diagnosis	current diagnosis	
previous diagnoses	medical history	
equipment info	physical medication	
	medication info	
medication dosage	physical medication	
	medication info	
medication name	physical medication	
	medication info	
tests to be performed	required test information	
lab results	lab results	

Table 9 - Representation of Information through Documents

### Structure of Information and Documents

Documents (information) are composed of other documents (information). Composition of documents (information) is captured through *part of* relations. This gives us an idea of how information and/or documents in the Sundhedsplatformen project are structured.

Table 10 and Table 11 summarises the information and documents in the Sundhedsplatformen project (Figure 2), showing how they are composed and describing the composition.

Information	Composition	Description
personal info	CPR-Number	

Table 10 - Information composition

Document	Composition	Description
outpatient record	treatment plan	
	current diagnosis	
treatment plan	medication info	
	treatment schedule	

Table 11 - Documents composition

## Authorization View

The authorization view shows the permissions or prohibitions flow from a stakeholder to another, that is, the authorizations stakeholders grant or deny to others about information, specifying the operations the others can and must perform over the information. Apart from granting authority on performing operations, a higher authority can be granted, that of further authorising other actors (i.e. authorization transferability)

Authorizations start from the information owner. Therefore, in the authorization view, ownership is preserved and inherited from the information view.

### Authorization View Diagram

Figure 3 presents the graphical representation of the Authorization view (a larger picture is represented in appendix A).

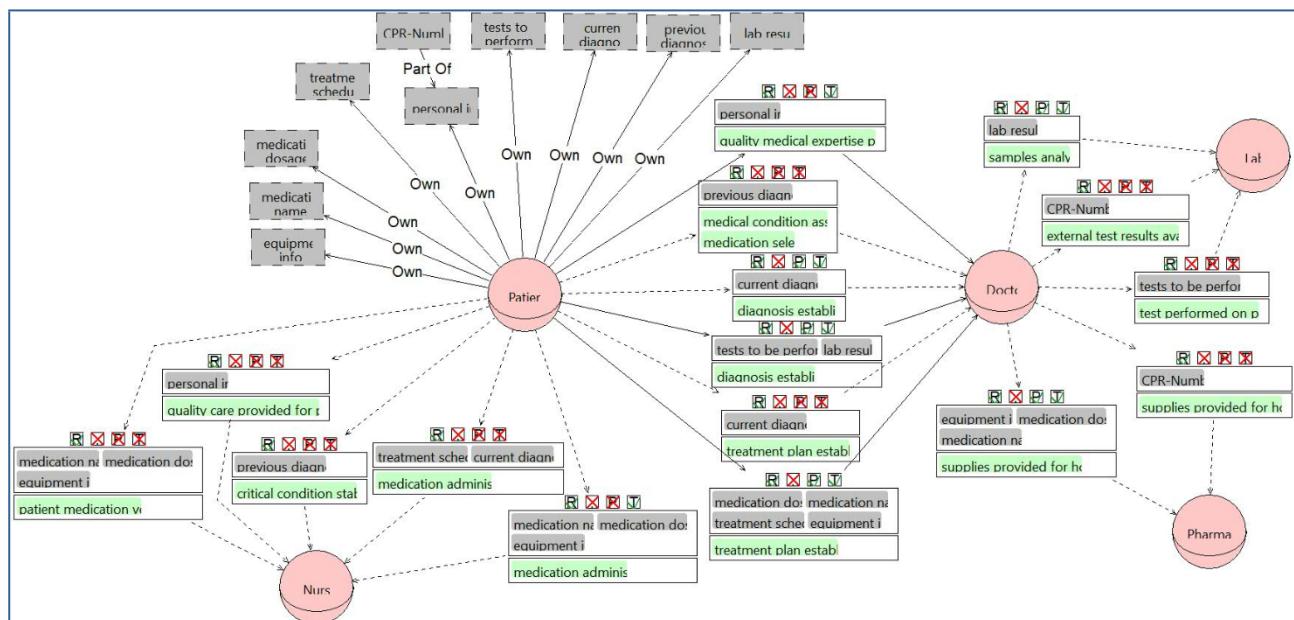


Figure 3 - Authorization View for the Sundhedsplatformen project

## Authorization Flow

In this section are described for each role/agent, the authorizations it passes to others and what authorizations it receives from other roles/agents. In the Sundhedsplatformen project (Figure 3) the authorizations for each role/agent are:

- **Role Patient:**
  - **Patient** authorises **Doctor** to *read* and *transmit* and prohibits to *modify* and *produce* information *personal info*, in the scope of goal *quality medical expertise provided*, passing the right to further authorising other actors, and authorises **Doctor** to *read*, *produce* and *transmit* and prohibits to *modify* information *medication dosage*, *medication name*, *treatment schedule* and *equipment info*, in the scope of goal *treatment plan established*, passing the right to further authorising other actors, and authorises **Doctor** to *read*, *produce* and *transmit* and prohibits to *modify* information *tests to be performed* and *lab results*, in the scope of goal *diagnosis established*, passing the right to further authorising other actors, and authorises **Doctor** to *read* and prohibits to *modify*, *produce* and *transmit* information *current diagnosis*, in the scope of goal *treatment plan established*, passing the right to further authorising other actors, and authorises **Nurse** to *read* and prohibits to *modify*, *produce* and *transmit* information *medication name*, *medication dosage* and *equipment info*, in the scope of goal *patient medication verified*, passing the right to further authorising other actors, and authorises **Nurse** to *read* and prohibits to *modify*, *produce* and *transmit* information *treatment schedule* and *current diagnosis*, in the scope of goal *medication administered*, passing the right to further authorising other actors, and authorises **Doctor** to *read*, *produce* and *transmit* and prohibits to *modify* information *current diagnosis*, in the scope of goal *diagnosis established*, passing the right to further authorising other actors, and authorises **Doctor** to *read* and prohibits to *modify*, *produce* and *transmit* information *previous diagnoses*, in the scope of goals *medical condition assessed* and *medication selected*, passing the right to further authorising other actors, and authorises **Nurse** to *read* and *transmit* and prohibits to *modify* and *produce* information *medication name*, *medication dosage* and *equipment info*, in the scope of goal *medication administered*, passing the right to further authorising other actors, and authorises **Nurse** to *read* and prohibits to *modify*, *produce* and *transmit* information *previous diagnoses*, in the scope of goal *critical condition stabilized*, passing the right to further authorising other actors, and authorises **Nurse** to *read* and prohibits to *modify*, *produce* and *transmit* information *personal info*, in the scope of goal *quality care provided for patients*, passing the right to further authorising other actors.
- **Role Doctor:**
  - **Doctor** authorises **Lab** to *read* and prohibits to *modify*, *produce* and *transmit* information *tests to be performed*, in the scope of goal *test performed on patient*, passing the right to further authorising other actors, and authorises **Lab** to *read*, *produce* and *transmit* and prohibits to *modify* information *lab results*, in the scope of goal *samples analyzed*, passing the right to further authorising other actors, and authorises **Pharmacy** to *read*, *produce* and *transmit* and prohibits to *modify* information *equipment info*, *medication dosage* and *medication name*, in the scope of goal *supplies provided for hospitals*, passing the right to further authorising other actors, and authorises **Lab** to *read* and prohibits to *modify*, *produce* and *transmit* information *CPR-Number*, in the scope of goal *external test results available*, passing the right to further authorising other actors, and authorises **Pharmacy** to *read* and

prohibits to *modify, produce and transmit* information *CPR-Number*, in the scope of goal *supplies provided for hospitals, passing* the right to further authorising other actors.

- **Doctor** is authorised by *Doctor* to *read and transmit* and prohibited to *modify and produce* information *personal info*, in the scope of goal *quality medical expertise provided, having* the right to further authorising other actors, and is authorised by *Doctor* to *read, produce and transmit* and prohibited to *modify* information *medication dosage, medication name, treatment schedule* and *equipment info*, in the scope of goal *treatment plan established, having* the right to further authorising other actors, and is authorised by *Doctor* to *read, produce and transmit* and prohibited to *modify* information *tests to be performed* and *lab results*, in the scope of goal *diagnosis established, having* the right to further authorising other actors, and is authorised by *Doctor* to *read and prohibited to modify, produce and transmit* information *current diagnosis*, in the scope of goal *treatment plan established, having* the right to further authorising other actors, and is authorised by *Doctor* to *read, produce and transmit* and prohibited to *modify* information *current diagnosis*, in the scope of goal *diagnosis established, having* the right to further authorising other actors, and is authorised by *Doctor* to *read and prohibited to modify, produce and transmit* information *previous diagnoses*, in the scope of goal *medical condition assessed* and *medication selected, having* the right to further authorising other actors.
- **Role Lab:**
  - **Lab** is authorised by *Lab* to *read* and prohibited to *modify, produce and transmit* information *tests to be performed*, in the scope of goal *test performed on patient, having* the right to further authorising other actors, and is authorised by *Lab* to *read, produce and transmit* and prohibited to *modify* information *lab results*, in the scope of goal *samples analyzed, having* the right to further authorising other actors, and is authorised by *Lab* to *read and prohibited to modify, produce and transmit* information *CPR-Number*, in the scope of goal *external test results available, having* the right to further authorising other actors.
- **Role Nurse:**
  - **Nurse** is authorised by *Nurse* to *read* and prohibited to *modify, produce and transmit* information *medication name, medication dosage* and *equipment info*, in the scope of goal *patient medication verified, having* the right to further authorising other actors, and is authorised by *Nurse* to *read and prohibited to modify, produce and transmit* information *treatment schedule* and *current diagnosis*, in the scope of goal *medication administered, having* the right to further authorising other actors, and is authorised by *Nurse* to *read and transmit* and prohibited to *modify and produce* information *medication name, medication dosage* and *equipment info*, in the scope of goal *medication administered, having* the right to further authorising other actors, and is authorised by *Nurse* to *read and prohibited to modify, produce and transmit* information *previous diagnoses*, in the scope of goal *critical condition stabilized, having* the right to further authorising other actors, and is authorised by *Nurse* to *read and prohibited to modify, produce and transmit* information *personal info*, in the scope of goal *quality care provided for patients, having* the right to further authorising other actors.
- **Role Pharmacy:**
  - **Pharmacy** is authorised by *Pharmacy* to *read, produce and transmit* and prohibited to *modify* information *equipment info, medication dosage* and *medication name*, in the scope of goal *supplies provided for hospitals, having* the right to further authorising other actors, and is



authorised by *Pharmacy* to *read* and prohibited to *modify, produce and transmit* information *CPR-Number*, in the scope of goal *supplies provided for hospitals, having the right to further authorising other actors.*

## Security Requirements

This section provides the list of security requirements derived for the Sundhedsplatformen project.

The list of security requirements shows the roles/agents that are *responsible* to satisfy them, so that stakeholders know what they have to bring about in order to satisfy the corresponding security needs. Security requirements also include the authorizations granted by stakeholders to other stakeholders.

*Security needs* are expressed mainly over goal delegations, document provisions and authorizations. Therefore, the list of security requirements is derived from every type of security need. Moreover, the organisational constraints specify further *needs* over roles and goal, leading to the generation of other security requirements.

Finally, the *requester* actors are represented to capture the actors requiring certain security needs to be brought about.

The security requirements for the Sundhedsplatformen project (Table 12) are:

- **Patient** requires *Doctor non-repudiation-of-acceptance* of the delegation of goal *diagnosis established*, when delegating *diagnosis established* to *Doctor*; while it is required by *Doctor delegator-authentication* when delegating *diagnosis established* to *Doctor*; while it requires *Nurse no-delegation* on goal *medication administered* and *non-repudiation-of-acceptance* of the delegation of goal *medication administered*, when delegating *medication administered* to *Nurse*; while it is required by *Nurse delegator-authentication* when delegating *medication administered* to *Nurse*; while it requires *Doctor non-repudiation-of-acceptance* of the delegation of goal *treatment plan established*, when delegating *treatment plan established* to *Doctor*; while it is required by *Doctor delegator-authentication* when delegating *treatment plan established* to *Doctor*; while it requires *Nurse non-repudiation-of-acceptance* of the delegation of goal *critical condition stabilized*, when delegating *critical condition stabilized* to *Nurse*.
- **Patient** requires *Doctor* a *receiver-authentication* and a *receiver-confidentiality*, when transmitting *medical history* to *Doctor* requires *Nurse* a *receiver-authentication* and a *receiver-confidentiality*, when transmitting *medical history* to *Nurse*.
- **Patient** requires *Doctor* the *non-modification* and *non-production* of information *personal info*, and *need-to-know* of these pieces of information for the goal *quality medical expertise provided*, when authorising *Doctor* to *read* and *distribute personal info* in the scope of goal *quality medical expertise provided*; while it requires *Doctor* the *non-modification* of information *medication dosage*, *medication name*, *treatment schedule* and *equipment info*, and *need-to-know* of these pieces of informations for the goal *treatment plan established*, when authorising *Doctor* to *read*, *produce* and *distribute medication dosage*, *medication name*, *treatment schedule* and *equipment info* in the scope of goal *treatment plan established*; while it requires *Doctor* the *non-modification* of information *tests to be performed* and *lab results*, and *need-to-know* of these pieces of informations for the goal *diagnosis established*, when authorising *Doctor* to *read*, *produce* and *distribute tests to be performed* and *lab results* in the scope of goal *diagnosis established*; while it requires *Doctor* the *non-modification*, *non-production* and *non-disclosure* of information *current diagnosis*, and *need-to-know* of these pieces of information for the goal *treatment plan established*, when authorising *Doctor* to *read current diagnosis* in the scope of goal *treatment plan established* not-reauthorised is required since the authorization is non-transferable; while it requires *Nurse* the *non-modification*, *non-production* and *non-disclosure* of information *medication name*, *medication dosage* and *equipment info*, and *need-to-know* of these pieces of informations for

the goal *patient medication verified*, when authorising *Nurse* to *read medication name, medication dosage* and *equipment info* in the scope of goal *patient medication verified*not-reauthorised is required since the authorization is non-transferable; while it requires *Nurse* the *non-modification, non-production* and *non-disclosure* of information *treatment schedule* and *current diagnosis*, and *need-to-know* of these pieces of informations for the goal *medication administered*, when authorising *Nurse* to *read treatment schedule* and *current diagnosis* in the scope of goal *medication administered*not-reauthorised is required since the authorization is non-transferable; while it requires *Doctor* the *non-modification* of information *current diagnosis*, and *need-to-know* of these pieces of information for the goal *diagnosis established*, when authorising *Doctor* to *read, produce* and *distribute current diagnosis* in the scope of goal *diagnosis established*not-reauthorised is required since the authorization is non-transferable; while it requires *Doctor* the *non-modification, non-production* and *non-disclosure* of information *previous diagnoses*, and *need-to-know* of these pieces of information for the goals *medical condition assessed* and *medication selected*, when authorising *Doctor* to *read previous diagnoses* in the scope of goals *medical condition assessed* and *medication selected*not-reauthorised is required since the authorization is non-transferable; while it requires *Nurse* the *non-modification* and *non-production* of information *medication name, medication dosage* and *equipment info*, and *need-to-know* of these pieces of informations for the goal *medication administered*, when authorising *Nurse* to *read and distribute medication name, medication dosage* and *equipment info* in the scope of goal *medication administered*not-reauthorised is required since the authorization is non-transferable; while it requires *Nurse* the *non-modification, non-production* and *non-disclosure* of information *previous diagnoses*, and *need-to-know* of these pieces of information for the goal *critical condition stabilized*, when authorising *Nurse* to *read previous diagnoses* in the scope of goal *critical condition stabilized*not-reauthorised is required since the authorization is non-transferable; while it requires *Nurse* the *non-modification, non-production* and *non-disclosure* of information *personal info*, and *need-to-know* of these pieces of information for the goal *quality care provided for patients*, when authorising *Nurse* to *read personal info* in the scope of goal *quality care provided for patients*not-reauthorised is required since the authorization is non-transferable.

- **Doctor** requires *Lab no-delegation* on goal *external test results available, non-repudiation-of-acceptance* of the delegation of goal *external test results available* and *delegatee-authentication* , when delegating *external test results available* to *Lab*; while it is required by *Lab non-repudiation-of-delegation* of the delegation of goal *external test results available*when delegating *external test results available* to *Lab*.
- **Doctor** requires *Patient a receiver-authentication* , when transmitting *outpatient record* to *Patient*; while it is required by *Patient a sender-confidentiality* when transmitting *outpatient record* to *Patient*requires *Lab a receiver-authentication* , when transmitting *required test information* to *Lab*, and *system confidentiality* is required for the transmission to take placerequires *Nurse a receiver-authentication* , when transmitting *treatment plan* to *Nurse*, and *system confidentiality* is required for the transmission to take placerequires *Nurse a receiver-authentication* , when transmitting *current diagnosis* to *Nurse*, and *system confidentiality* is required for the transmission to take placerequires *Pharmacy a receiver-authentication* , when transmitting *medication info* to *Pharmacy*, and *system confidentiality* is required for the transmission to take placerequires *Nurse a receiver-authentication* , when transmitting *medication info* to *Nurse*, and *system confidentiality* is required for the transmission to take place.
- **Doctor** requires *Lab the non-modification, non-production* and *non-disclosure* of information *tests to be performed*, and *need-to-know* of these pieces of information for the goal *test performed on*

patient, when authorising *Lab* to *read tests to be performed* in the scope of goal *test performed on patient* not-reauthorised is required since the authorization is non-transferable; while it requires *Lab* the *non-modification* of information *lab results*, and *need-to-know* of these pieces of information for the goal *samples analyzed*, when authorising *Lab* to *read, produce and distribute lab results* in the scope of goal *samples analyzed* not-reauthorised is required since the authorization is non-transferable; while it requires *Pharmacy* the *non-modification* of information *equipment info, medication dosage* and *medication name*, and *need-to-know* of these pieces of informations for the goal *supplies provided for hospitals*, when authorising *Pharmacy* to *read, produce and distribute equipment info, medication dosage* and *medication name* in the scope of goal *supplies provided for hospitals* not-reauthorised is required since the authorization is non-transferable; while it requires *Lab* the *non-modification, non-production* and *non-disclosure* of information *CPR-Number*, and *need-to-know* of these pieces of information for the goal *external test results available*, when authorising *Lab* to *read CPR-Number* in the scope of goal *external test results available* not-reauthorised is required since the authorization is non-transferable; while it requires *Pharmacy* the *non-modification, non-production* and *non-disclosure* of information *CPR-Number*, and *need-to-know* of these pieces of information for the goal *supplies provided for hospitals*, when authorising *Pharmacy* to *read CPR-Number* in the scope of goal *supplies provided for hospitals* not-reauthorised is required since the authorization is non-transferable.

- **Lab** requires *Doctor* a *receiver-authentication*, when transmitting *lab results* to *Doctor*, and *system confidentiality* and *system integrity* are required for the transmission to take place.
- **Nurse** requires *Pharmacy* *no-delegation* on goal *patient medication prepared, non-repudiation-of-acceptance* of the delegation of goal *patient medication prepared* and *delegatee-authentication*, when delegating *patient medication prepared* to *Pharmacy*; while it is required by *Pharmacy* *non-repudiation-of-delegation* of the delegation of goal *patient medication prepared* when delegating *patient medication prepared* to *Pharmacy*; while it requires *Pharmacy* *no-delegation* on goal *medical equipment provided, non-repudiation-of-acceptance* of the delegation of goal *medical equipment provided* and *delegatee-authentication*, when delegating *medical equipment provided* to *Pharmacy*; while it is required by *Pharmacy* *non-repudiation-of-delegation* of the delegation of goal *medical equipment provided* when delegating *medical equipment provided* to *Pharmacy*.
- **Nurse** requires *Patient* a *receiver-authentication*, when transmitting *physical medication* to *Patient*; while it is required by *Patient* a *sender-confidentiality* when transmitting *physical medication* to *Patient*.
- **Pharmacy** requires *Nurse* a *receiver-authentication*, when transmitting *physical medication* to *Nurse*, and *system confidentiality* and *system integrity* are required for the transmission to take place.

<b>Responsible</b>	<b>Security Requirement</b>	<b>Requester</b>	<b>Description</b>
Patient	delegator-authentication (delegated(Doctor,Patient,diagnosis established))	Patient	Doctor require Patient to be authenticated in order to delegate the goal diagnosis established.
	delegator-authentication (delegated(Nurse,Patient, medication)	Patient	Nurse require Patient to be authenticated in order to delegate the goal

	administered))		medication administered.
	delegator-authentication (delegated(Doctor,Patient,treatment plan established))	Patient	Doctor require Patient to be authenticated in order to delegate the goal treatment plan established.
	receiver-authentication (transmitted(Patient,Doctor,outpatient record))	Doctor	Doctor require Patient to authenticate in order to receive document outpatient record.
	receiver-authentication (transmitted(Patient,Nurse,physical medication))	Nurse	Nurse require Patient to authenticate in order to receive document physical medication.
	non-repudiation-of-acceptance (delegated(Patient,Doctor,diagnosis established))	Patient	Patient require non-repudiation-of-acceptance for goal diagnosis established,when delegating diagnosis established to Doctor.
	non-repudiation-of-acceptance (delegated(Patient,Doctor,treatment plan established))	Patient	Patient require non-repudiation-of-acceptance for goal treatment plan established,when delegating treatment plan established to Doctor.
	non-repudiation-of-delegation (delegated(Doctor,Lab,external test results available))	Lab	Lab require non-repudiation-of-delegation for goal external test results available,when delegated external test results available by Doctor.
	receiver-authentication (transmitted(Doctor,Lab,lab results))	Lab	Lab require Doctor to authenticate in order to receive document lab results.
Doctor	receiver-authentication (transmitted(Doctor,Patient,medical history))	Patient	Patient require Doctor to authenticate in order to receive document medical history.
	reciever-confidentiality (transmitted(Patient,Doctor,medical history))	Patient	Doctor shall ensure the confidentiality of transmission of the document medical history being transmitted.
	sender-confidentiality (transmitted(Doctor,Patient,outpatient record))	Patient	Doctor shall ensure the confidentiality of transmission of the document outpatient record while being transmitted.
	non-modification (personal info)	Patient	Patient requires Doctor non-modification of Information personal info.
	non-production (personal info)	Patient	Patient requires Doctor non-production of Information personal info.
	need-to-know (personal info)	Patient	Patient requires Doctor need-to-know of

(quality medical expertise provided)	Patient	Information personal info, in the scope of goal quality medical expertise provided.
non-modification (medication dosage, medication name, treatment schedule, equipment info)	Patient	Patient requires Doctor non-modification of Information medication dosage, medication name, treatment schedule and equipment info.
need-to-know (medication dosage, medication name, treatment schedule, equipment info) (treatment plan established)	Patient	Patient requires Doctor need-to-know of Information medication dosage, medication name, treatment schedule and equipment info, in the scope of goal treatment plan established.
non-modification (tests to be performed, lab results)	Patient	Patient requires Doctor non-modification of Information tests to be performed and lab results.
need-to-know (tests to be performed, lab results) (diagnosis established)	Patient	Patient requires Doctor need-to-know of Information tests to be performed and lab results, in the scope of goal diagnosis established.
non-modification (current diagnosis)	Patient	Patient requires Doctor non-modification of Information current diagnosis.
non-production (current diagnosis)	Patient	Patient requires Doctor non-production of Information current diagnosis.
non-disclosure (current diagnosis)	Patient	Patient requires Doctor non-disclosure of Information current diagnosis.
need-to-know (current diagnosis) (treatment plan established)	Patient	Patient requires Doctor need-to-know of Information current diagnosis, in the scope of goal treatment plan established.
not-reauthorized ({current diagnosis}, {treatment plan established}, {R})	Patient	Patient wants Doctor not to redistribute permissions on information {current diagnosis} to other actors.
non-modification (current diagnosis)	Patient	Patient requires Doctor non-modification of Information current diagnosis.
need-to-know (current diagnosis) (diagnosis established)	Patient	Patient requires Doctor need-to-know of Information current diagnosis, in the scope of goal diagnosis established.

	not-reauthorized ({current diagnosis},{diagnosis established},{R})	Patient	Patient wants Doctor not to redistribute permissions on information {current diagnosis} to other actors.
	not-reauthorized ({current diagnosis},{diagnosis established},{P})	Patient	Patient wants Doctor not to redistribute permissions on information {current diagnosis} to other actors.
	not-reauthorized ({current diagnosis},{diagnosis established},{T})	Patient	Patient wants Doctor not to redistribute permissions on information {current diagnosis} to other actors.
	non-modification (previous diagnoses)	Patient	Patient requires Doctor non-modification of Information previous diagnoses.
	non-production (previous diagnoses)	Patient	Patient requires Doctor non-production of Information previous diagnoses.
	non-disclosure (previous diagnoses)	Patient	Patient requires Doctor non-disclosure of Information previous diagnoses.
	need-to-know (previous diagnoses) (medical condition assessed, medication selected)	Patient	Patient requires Doctor need-to-know of Information previous diagnoses, in the scope of goal medical condition assessed and medication selected.
	not-reauthorized ({previous diagnoses},{medical condition assessed, medication selected},{R})	Patient	Patient wants Doctor not to redistribute permissions on information {previous diagnoses} to other actors.
Lab	no-delegation (external test results available)	Doctor	Lab requires no-delegation for goal external test results available, when delegating external test results available to Lab.
	non-repudiation-of-acceptance (delegated(Doctor,Lab,external test results available))	Doctor	Doctor require non-repudiation-of-acceptance for goal external test results available, when delegating external test results available to Lab.
	delegatee-authentication (delegated(Doctor,Lab,external test results available))	Doctor	Doctor require Lab to authenticate in order to achieve goal external test results available.
	receiver-authentication (transmitted(Lab,Doctor, required test information))	Doctor	Doctor require Lab to authenticate in order to receive document required test information.

non-modification (tests to be performed)	Doctor	Doctor requires Lab non-modification of Information tests to be performed.
non-production (tests to be performed)	Doctor	Doctor requires Lab non-production of Information tests to be performed.
non-disclosure (tests to be performed)	Doctor	Doctor requires Lab non-disclosure of Information tests to be performed.
need-to-know (tests to be performed) (test performed on patient)	Doctor	Doctor requires Lab need-to-know of Information tests to be performed, in the scope of goal test performed on patient.
not-reauthorized ({tests to be performed},{test performed on patient},{R})	Doctor	Doctor wants Lab not to redistribute permissions on information {tests to be performed} to other actors.
non-modification (lab results)	Doctor	Doctor requires Lab non-modification of Information lab results.
need-to-know (lab results) (samples analyzed)	Doctor	Doctor requires Lab need-to-know of Information lab results, in the scope of goal samples analyzed.
not-reauthorized ({lab results},{samples analyzed},{R})	Doctor	Doctor wants Lab not to redistribute permissions on information {lab results} to other actors.
not-reauthorized ({lab results},{samples analyzed},{P})	Doctor	Doctor wants Lab not to redistribute permissions on information {lab results} to other actors.
not-reauthorized ({lab results},{samples analyzed},{T})	Doctor	Doctor wants Lab not to redistribute permissions on information {lab results} to other actors.
non-modification (CPR-Number)	Doctor	Doctor requires Lab non-modification of Information CPR-Number.
non-production (CPR-Number)	Doctor	Doctor requires Lab non-production of Information CPR-Number.
non-disclosure (CPR-Number)	Doctor	Doctor requires Lab non-disclosure of Information CPR-Number.
need-to-know (CPR-Number) (external test results available)	Doctor	Doctor requires Lab need-to-know of Information CPR-Number, in the scope of goal external test results available.
not-reauthorized ({CPR-Number},{external test results available},{R})	Doctor	Doctor wants Lab not to redistribute permissions on information {CPR-Number} to other actors.

Nurse	no-delegation (medication administered)	Patient	Nurse requires no-delegation for goal medication administered,when delegating medication administered to Nurse.
	non-repudiation-of-acceptance (delegated(Patient,Nurse, medication administered))	Patient	Patient require non-repudiation-of-acceptance for goal medication administered,when delegating medication administered to Nurse.
	non-repudiation-of-acceptance (delegated(Patient,Nurse, critical condition stabilized))	Patient	Patient require non-repudiation-of-acceptance for goal critical condition stabilized,when delegating critical condition stabilized to Nurse.
	non-repudiation-of-delegation (delegated(Nurse,Pharmacy,patient medication prepared))	Pharmacy	Pharmacy require non-repudiation-of-delegation for goal patient medication prepared,when delegated patient medication prepared by Nurse.
	non-repudiation-of-delegation (delegated(Nurse,Pharmacy,medical equipment provided))	Pharmacy	Pharmacy require non-repudiation-of-delegation for goal medical equipment provided,when delegated medical equipment provided by Nurse.
	receiver-authentication (transmitted(Nurse,Pharmacy,physical medication))	Pharmacy	Pharmacy require Nurse to authenticate in order to receive document physical medication.
	receiver-authentication (transmitted(Nurse,Doctor,treatment plan))	Doctor	Doctor require Nurse to authenticate in order to receive document treatment plan.
	receiver-authentication (transmitted(Nurse,Doctor,current diagnosis))	Doctor	Doctor require Nurse to authenticate in order to receive document current diagnosis.
	receiver-authentication (transmitted(Nurse,Patient,medical history))	Patient	Patient require Nurse to authenticate in order to receive document medical history.
	reciever-confidentiality (transmitted(Patient,Nurse,medical history))	Patient	Nurse shall ensure the confidentiality of transmission of the document medical history being transmitted.
	receiver-authentication (transmitted(Nurse,Doctor,medication info))	Doctor	Doctor require Nurse to authenticate in order to receive document medication info.
	sender-confidentiality (transmitted(Nurse,Patient,physical medication))	Patient	Nurse shall ensure the confidentiality of transmission of the document physical

			medication while being transmitted.
non-modification (medication name, medication dosage, equipment info)	Patient	Patient requires Nurse non-modification of Information medication name, medication dosage and equipment info.	
non-production (medication name, medication dosage, equipment info)	Patient	Patient requires Nurse non-production of Information medication name, medication dosage and equipment info.	
non-disclosure (medication name, medication dosage, equipment info)	Patient	Patient requires Nurse non-disclosure of Information medication name, medication dosage and equipment info.	
need-to-know (medication name, medication dosage, equipment info) (patient medication verified)	Patient	Patient requires Nurse need-to-know of Information medication name, medication dosage and equipment info, in the scope of goal patient medication verified.	
not-reauthorized ({{medication name, medication dosage, equipment info}}, {patient medication verified}, {R})	Patient	Patient wants Nurse not to redistribute permissions on information {{medication name, medication dosage, equipment info}} to other actors.	
non-modification (treatment schedule, current diagnosis)	Patient	Patient requires Nurse non-modification of Information treatment schedule and current diagnosis.	
non-production (treatment schedule, current diagnosis)	Patient	Patient requires Nurse non-production of Information treatment schedule and current diagnosis.	
non-disclosure (treatment schedule, current diagnosis)	Patient	Patient requires Nurse non-disclosure of Information treatment schedule and current diagnosis.	
need-to-know (treatment schedule, current diagnosis) (medication administered)	Patient	Patient requires Nurse need-to-know of Information treatment schedule and current diagnosis, in the scope of goal medication administered.	
not-reauthorized ({{treatment schedule, current diagnosis}}, {medication administered}, {R})	Patient	Patient wants Nurse not to redistribute permissions on information {{treatment schedule, current diagnosis}} to other actors.	
non-modification (medication	Patient	Patient requires Nurse non-modification of Information	

name,medication dosage,equipment info)	Patient	medication name, medication dosage and equipment info.
non-production (medication name,medication dosage,equipment info)	Patient	Patient requires Nurse non- production of Information medication name, medication dosage and equipment info.
need-to-know (medication name,medication dosage,equipment info) (medication administered)	Patient	Patient requires Nurse need-to-know of Information medication name, medication dosage and equipment info, in the scope of goal medication administered.
not-reauthorized ({medication name,medication dosage,equipment info},{medication administered},{R})	Patient	Patient wants Nurse not to redistribute permissions on information {medication name,medication dosage,equipment info} to other actors.
not-reauthorized ({medication name,medication dosage,equipment info},{medication administered},{T})	Patient	Patient wants Nurse not to redistribute permissions on information {medication name,medication dosage,equipment info} to other actors.
non-modification (previous diagnoses)	Patient	Patient requires Nurse non- modification of Information previous diagnoses.
non-production (previous diagnoses)	Patient	Patient requires Nurse non- production of Information previous diagnoses.
non-disclosure (previous diagnoses)	Patient	Patient requires Nurse non- disclosure of Information previous diagnoses.
need-to-know (previous diagnoses) (critical condition stabilized)	Patient	Patient requires Nurse need-to-know of Information previous diagnoses, in the scope of goal critical condition stabilized.
not-reauthorized ({previous diagnoses},{critical condition stabilized},{R})	Patient	Patient wants Nurse not to redistribute permissions on information {previous diagnoses} to other actors.
non-modification (personal info)	Patient	Patient requires Nurse non- modification of Information personal info.
non-production (personal info)	Patient	Patient requires Nurse non- production of Information personal info.
non-disclosure (personal info)	Patient	Patient requires Nurse non- disclosure of Information personal info.
need-to-know	Patient	Patient requires Nurse

	(personal info) (quality care provided for patients)		need-to-know of Information personal info, in the scope of goal quality care provided for patients.
	not-reauthorized ({personal info},{quality care provided for patients},{R})	Patient	Patient wants Nurse not to redistribute permissions on information {personal info} to other actors.
	no-delegation (patient medication prepared)	Nurse	Pharmacy requires no- delegation for goal patient medication prepared,when delegating patient medication prepared to Pharmacy.
	non-repudiation-of- acceptance (delegated(Nurse,Pharm acy,patient medication prepared))	Nurse	Nurse require non- repudiation-of-acceptance for goal patient medication prepared,when delegating patient medication prepared to Pharmacy.
	delegatee-authentication (delegated(Nurse,Pharm acy,patient medication prepared))	Nurse	Nurse require Pharmacy to authenticate in order to achieve goal patient medication prepared.
Pharmacy	no-delegation (medical equipment provided)	Nurse	Pharmacy requires no- delegation for goal medical equipment provided,when delegating medical equipment provided to Pharmacy.
	non-repudiation-of- acceptance (delegated(Nurse,Pharm acy,medical equipment provided))	Nurse	Nurse require non- repudiation-of-acceptance for goal medical equipment provided,when delegating medical equipment provided to Pharmacy.
	delegatee-authentication (delegated(Nurse,Pharm acy,medical equipment provided))	Nurse	Nurse require Pharmacy to authenticate in order to achieve goal medical equipment provided.
	receiver-authentication (transmitted(Pharmacy, Doctor,medication info))	Doctor	Doctor require Pharmacy to authenticate in order to receive document medication info.
	non-modification (equipment info,medication dosage,medication name)	Doctor	Doctor requires Pharmacy non-modification of Information equipment info, medication dosage and medication name.
	need-to-know (equipment info,medication dosage,medication name) (supplies provided for hospitals)	Doctor	Doctor requires Pharmacy need-to-know of Information equipment info, medication dosage and medication name, in the scope of goal supplies provided for hospitals.
	not-reauthorized	Doctor	Doctor wants Pharmacy not to redistribute permissions

	$\{\{equipment\ info, medication\ dosage, medication\ name\}, \{supplies\ provided\ for\ hospitals\}, \{R\}\}$		on information {equipment info,medication dosage,medication name} to other actors.
	not-reauthorized $\{\{equipment\ info, medication\ dosage, medication\ name\}, \{supplies\ provided\ for\ hospitals\}, \{P\}\}$	Doctor	Doctor wants Pharmacy not to redistribute permissions on information {equipment info,medication dosage,medication name} to other actors.
	not-reauthorized $\{\{equipment\ info, medication\ dosage, medication\ name\}, \{supplies\ provided\ for\ hospitals\}, \{T\}\}$	Doctor	Doctor wants Pharmacy not to redistribute permissions on information {equipment info,medication dosage,medication name} to other actors.
	non-modification (CPR-Number)	Doctor	Doctor requires Pharmacy non-modification of Information CPR-Number.
	non-production (CPR-Number)	Doctor	Doctor requires Pharmacy non-production of Information CPR-Number.
	non-disclosure (CPR-Number)	Doctor	Doctor requires Pharmacy non-disclosure of Information CPR-Number.
	need-to-know (CPR-Number) (supplies provided for hospitals)	Doctor	Doctor requires Pharmacy need-to-know of Information CPR-Number, in the scope of goal supplies provided for hospitals.
	not-reauthorized $\{\{CPR\ Number\}, \{supplies\ provided\ for\ hospitals\}, \{R\}\}$	Doctor	Doctor wants Pharmacy not to redistribute permissions on information {CPR-Number} to other actors.
"The System"	system-integrity (transmitted(Pharmacy, Nurse,physical medication))	-	The system shall ensure the integrity of the transmitted document physical medication transmitted from Pharmacy to Nurse is preserved
"The System"	system-integrity (transmitted(Lab,Doctor, lab results))	-	The system shall ensure the integrity of the transmitted document lab results transmitted from Lab to Doctor is preserved
"The System"	system-confidentiality (transmitted(Pharmacy, Nurse,physical medication))	-	The system shall ensure the confidentiality of the transmitted document physical medication is

		preserved.
system-confidentiality (transmitted(Doctor,Nurse,treatment plan))	-	The system shall ensure the confidentiality of the transmitted document treatment plan is preserved.
system-confidentiality (transmitted(Lab,Doctor, lab results))	-	The system shall ensure the confidentiality of the transmitted document lab results is preserved.
system-confidentiality (transmitted(Doctor,Pharmacy,medication info))	-	The system shall ensure the confidentiality of the transmitted document medication info is preserved.
system-confidentiality (transmitted(Doctor,Nurse,medication info))	-	The system shall ensure the confidentiality of the transmitted document medication info is preserved.
system-confidentiality (transmitted(Doctor,Nurse,current diagnosis))	-	The system shall ensure the confidentiality of the transmitted document current diagnosis is preserved.
system-confidentiality (transmitted(Doctor,Lab, required test information))	-	The system shall ensure the confidentiality of the transmitted document required test information is preserved.

Table 12 - Security Requirements for the Sundhedsplatformen Project

Table 13 summarises the authorizations actors in the Sundhedsplatformen project grant to one another.

Authorisor Information	Goal	Allowed Operations	Denied Operations	Authorisee	Description
personal info	quality medical expertise provided	R, T	M, P	Doctor	Transferable authority
Patient	medication dosage medication name treatment schedule equipment info	treatment plan established	R, P, T	M	Doctor
	tests to be	diagnosis	R, P, T	M	Doctor
					Transferable

	performed lab results	established			authority
	current diagnosis	treatment plan established	R	M, P, T	Doctor Non-transferable authority
	medication name medication dosage equipment info	patient medication verified	R	M, P, T	Nurse Non-transferable authority
	treatment schedule current diagnosis	medication administered	R	M, P, T	Nurse Non-transferable authority
	current diagnosis	diagnosis established	R, P, T	M	Doctor Non-transferable authority
	previous diagnoses	medical condition assessed medication selected	R	M, P, T	Doctor Non-transferable authority
	medication name medication dosage equipment info	medication administered	R, T	M, P	Nurse Non-transferable authority
	previous diagnoses	critical condition stabilized	R	M, P, T	Nurse Non-transferable authority
	personal info	quality care provided for patients	R	M, P, T	Nurse Non-transferable authority
	tests to be performed	test performed on patient	R	M, P, T	Lab Non-transferable authority
	lab results	samples analyzed	R, P, T	M	Lab Non-transferable authority
Doctor	equipment info medication dosage medication name	supplies provided for hospitals	R, P, T	M	Pharmacy Non-transferable authority
	CPR-Number	external test results available	R	M, P, T	Lab Non-transferable authority
	CPR-Number	supplies provided for	R	M, P, T	Pharmacy Non-transferable

hospitals

authority

---

*Table 13 - Authorizations in the Sundhedsplatformen project*

## Well-formedness Analysis

The purpose of well-formedness analysis is to verify whether the diagram for the project Sundhedsplatformen is consistent and valid. A diagram is considered to be consistent if its constituent elements (concepts and relationships) are drawn and interconnected following the semantics of the modelling language (STS-ml in our case). Thus, well-formedness analysis performs post checks to verify compliance with STS-ml semantics for all checks that cannot be performed live over the models.

More details about the performed checks and their purpose can be found in Appendix B.

*The Well-formedness Analysis analysis for Sundhedsplatformen project didn't find any errors.*

## Security Analysis

The purpose of security analysis is to verify whether the diagram for the project Sundhedsplatformen allows the satisfaction of the specified security needs or not. As a result, for all security needs expressed by stakeholders, it checks in the model whether there is any possibility for the security need to be violated. This analysis takes into account the semantics of STS-ml, defining the behaviour of the different elements represented in the models. The elements' behaviour is defined by propagation rules that consider what concepts and what relationships the specification of a given security need affects. Datalog is used to define the semantics of STS-ml to express facts (things always hold) and rules.

You can find more details about the performed checks in Appendix C.

*The Security Analysis analysis for Sundhedsplatformen project didn't find any errors.*

## Appendix A

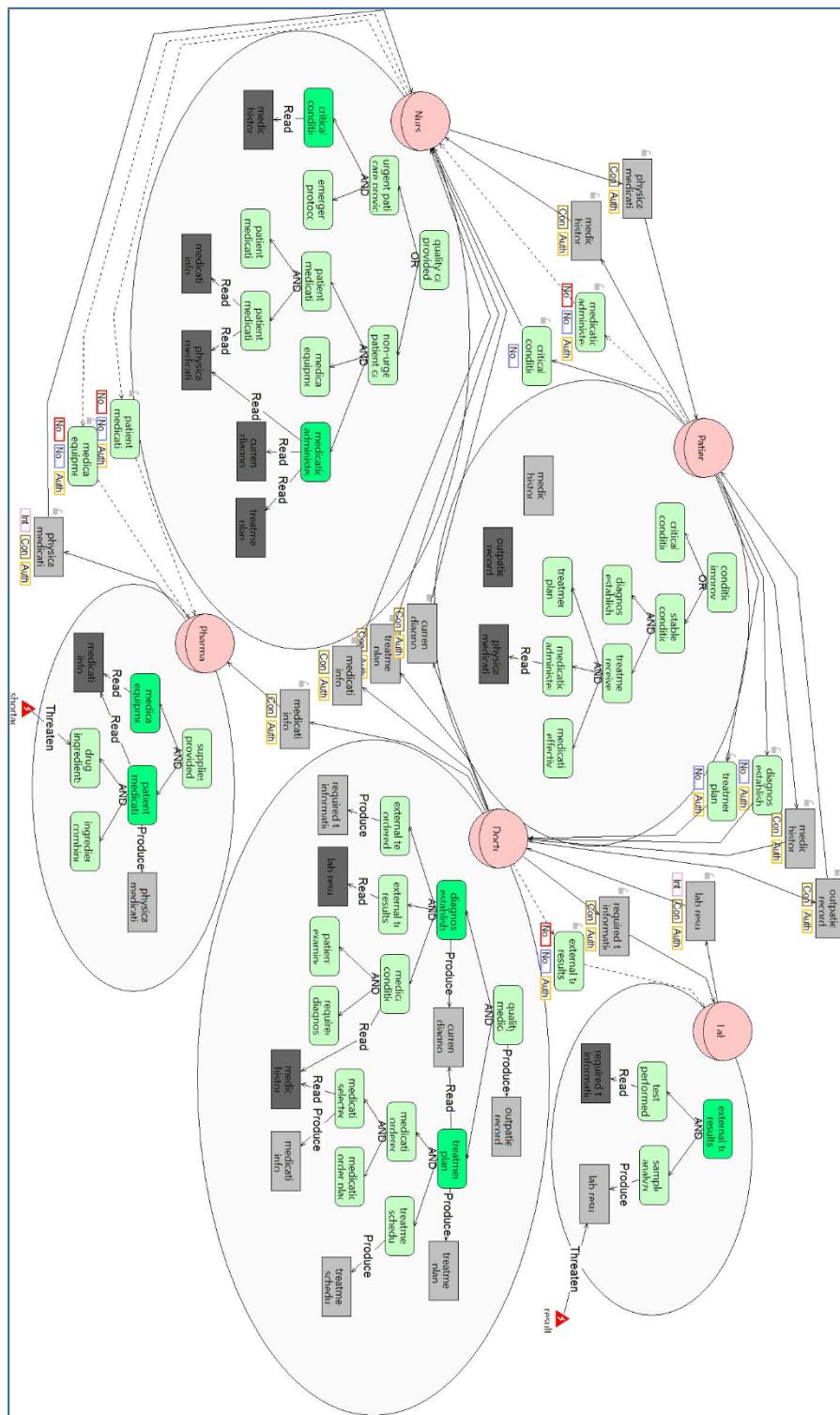


Figure 1 - Social View for the Sundhedsplatformen project

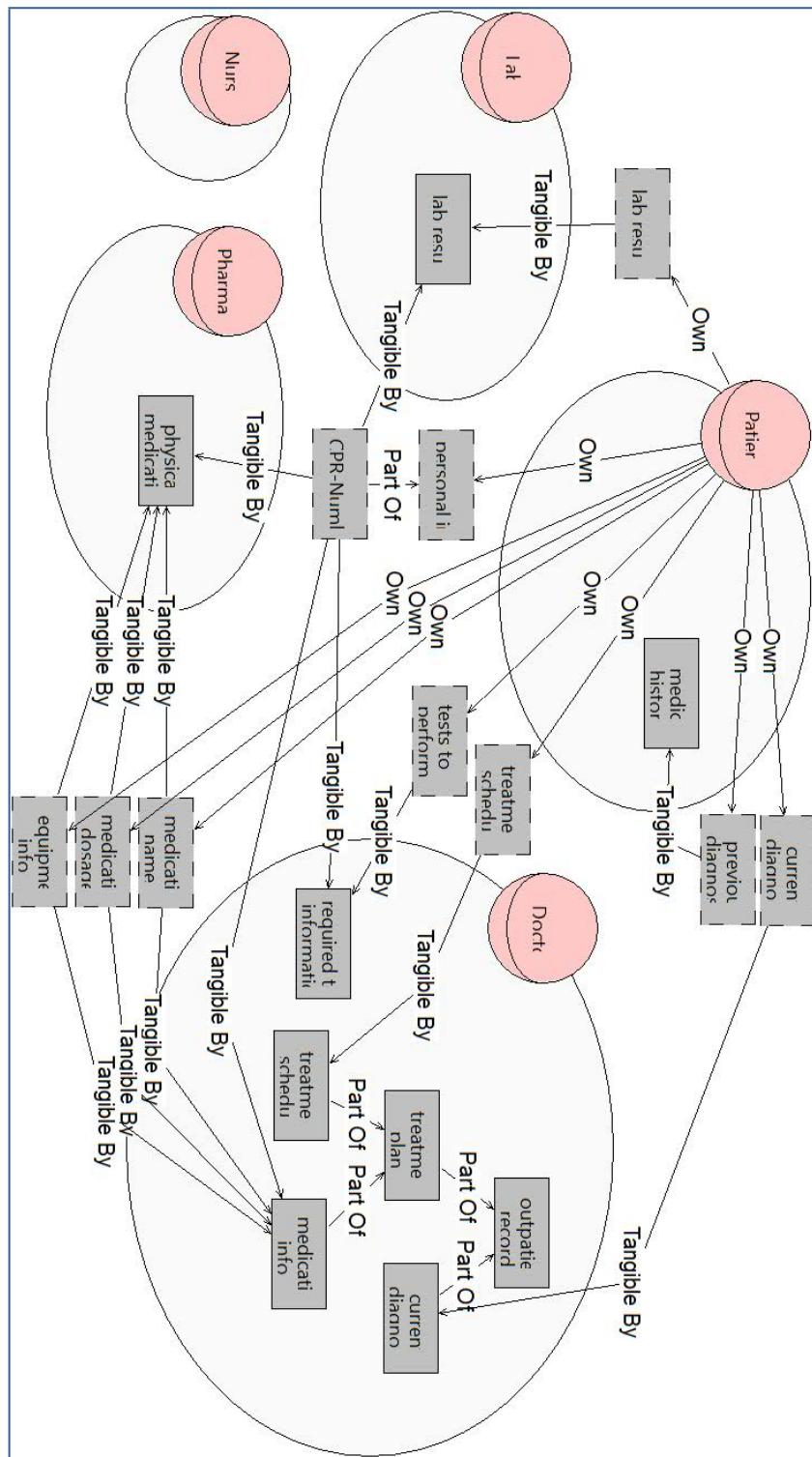
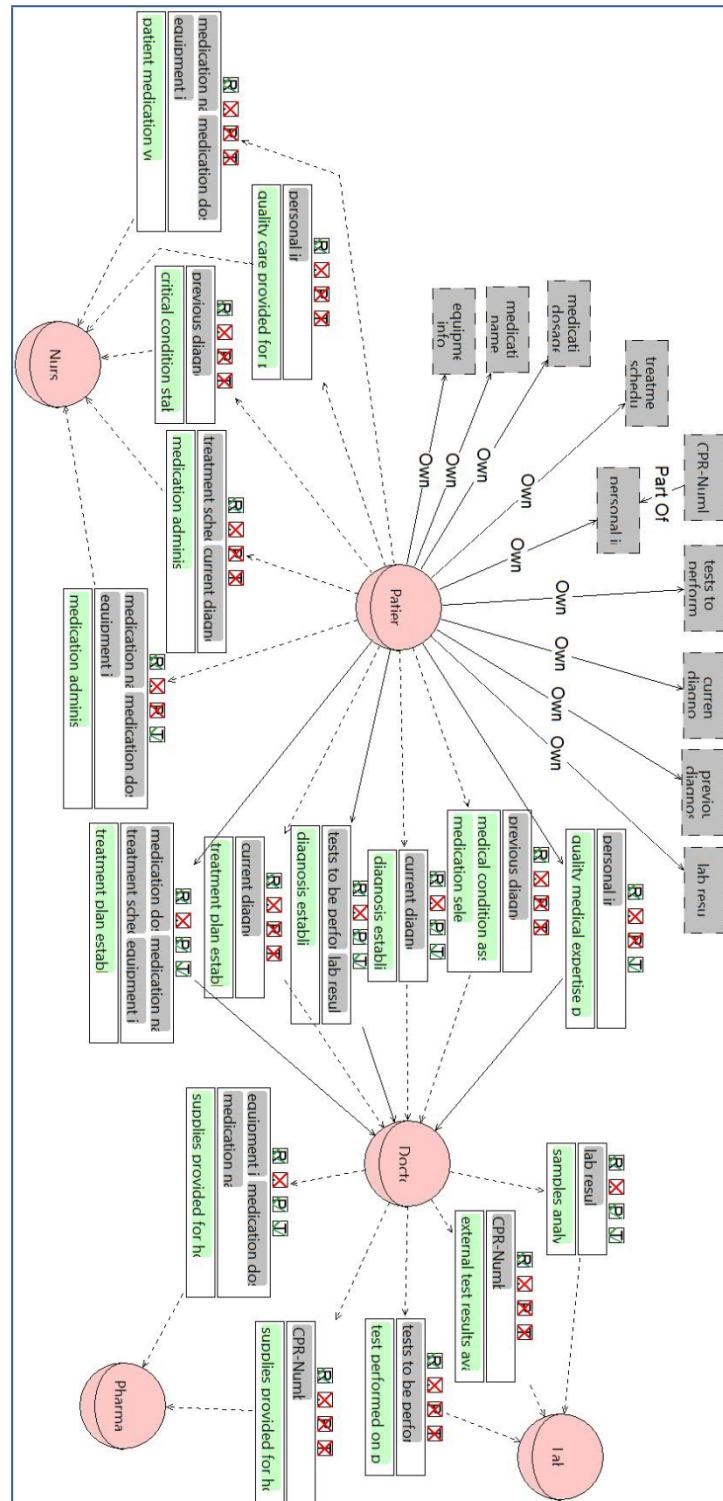


Figure 2 - Information View for the Sundhedsplatformen project



*Figure 3 - Authorization View for the Sundhedsplatformen project*

## Appendix B

Details of Well-formedness analysis:

- **Empty Diagram**

This check verifies whether the given diagram is empty or not. If that is the case, then no other well-formedness checks are performed. If the diagram is not empty, the well-formedness analysis returns: "No errors found" and continues performing the rest of the well-formedness checks.

- **Goal Single Decomposition**

This check verifies the consistency of goal decompositions. Following the semantics of STS-ml a given goal is decomposed in two or more subgoals. As a result, the decomposition should specify at least two subgoals. Therefore, goal single decomposition verifies whether there are cases of decompositions to a single subgoal.

- **Delegation Child Cycle**

This check verifies the consistency of goal delegations, so that no cycles or loops are identified as a result of the delegatee decomposing the delegatum (delegated goal) and re-delegating back one of the subgoals. Delegation child cycle verifies exactly this and gives a warning in case of inconsistency.

- **Delegated Goal Part Of a Decomposition**

This check verifies that all goals (in the delegatee's scope) that have been delegated are not child (subgoals) in the decomposition.

- **Inconsistent Contribution Cycle**

This check verifies whether there are loops of positive or negative contribution relationships, and whether this loop contains contradictory relationships. If such a loop is identified, the well-formedness analysis returns a warning.

- **Negative Contributions Between AND Subgoals**

This check verifies that there are no negative contribution relationships between and-subgoals of a given goal (within an actor's scope). It returns a warning if such a case is identified.

- **Documents PartOf Cycle**

This check verifies whether there is a loop or cycle of Part Of relationships starting from and ending to a given document. If a case like this is verified, a warning is returned enumerating the documents that form the cycle.

- **Informations PartOf Cycle**

This check verifies whether there is a loop or cycle of Part Of relationships starting from and ending to a given document. If a case like this is verified, a warning is returned enumerating the documents that form the cycle.

- **Information No Ownership**

This check verifies that all information have an owner. If there are cases of information without any ownership relationships from any actor in the diagram, the well-formedness analysis returns a warning.

- **Authorizations Validity**

This check verifies that all authorization relationship between two given actors are valid. An authorization relationship specifies authorizations or permissions an actor grants to another on some information, to perform some allowed operations. The authorizations could be limited to a goal scope and they can be re-delegated or not. However, the first two attributes should be specified for an authorization relationship to be valid. If there are no information specified, the well-formedness analysis returns an error. The same applies to the cases, in which no allowed operations are specified.

- **Duplicate Authorizations**

This check verifies that there are no duplicate authorization relationships, that could be merged. There are several cases that are addressed by this check: (i) we encounter two identical authorization, i.e., between the same roles, in the same direction, for the same set of information, allowed operations and goals, and having the same value of transferability; (ii) identify authorization relationships between the same roles, in the same direction, in which one grants permissions that are subset of the other authorization's relationship.

## Appendix C

Details of security analysis:

- **No\_Delegation Violation check**

This violation is verified whenever a delegatee actor further delegates a goal, over the delegation of which a no-delegation security need is specified from the delegator actor. No-delegation is specified over a goal delegation by the delegator, who requires the delegatee not to further delegate the delegated goal. Therefore, to check for any violations of no-delegation, the analysis searches for redelegations of the delegatum (delegated goal) or any of its subgoals.

- **Redundancy Violation check**

This check verifies if redundancy is satisfied by controlling that single actor redundancy or multi actor redundancy are not violated. At design time we cannot make the distinction between fallback and true redundancy, so they cannot be verified at this stage. Therefore, both fallback redundancy single and true redundancy single are mapped to single actor redundancy. Similarly for multi actor redundancy. The analysis verifies a redundancy violation if one of the following occurs: (1) actor does not decompose the delegated goal in any or-subgoals, for which both types of redundancy are violated (2) actor decomposes the goal into or-subgoals and delegates one to another actor when single actor redundancy has been specified, for which this type of redundancy is violated (3) actor decomposes the goal into or-subgoals, but does not delegate any of the subgoals to another actor when multi actor redundancy has been specified, for which this type of redundancy is violated.

- **Authorization Conflict check**

This task identifies a conflict of authorization whenever at least two authorization relationships for the same information are drawn towards the same actor from two illegible actors (being the owner of information or another authorised actor) such that: (1) one limits the authorization to a goal scope (requiring a need-to-know security need) and the other does not (authorising the actor without any limitations) (2) for the same goals or intersecting goal scopes, different permissions are granted in terms of operations or authority to transfer authoristaion. That is, one passes the actor the authority to perform operations (use, modify, produce, distribute) on a given information, and the other does not (requiring non-usage, non-modification, non-production, non-disclosure); one passes the actor the authority to further transfer authorizations and the other requires no further authorizations take place.

- **Non\_Reading Violation**

This violation is detected whenever an actor discloses information without having the right to distribute it. Non-disclosure expresses the need of not disclosing or further distributing the given information to other actors, apart from the authoriser. Thus, authority to distribute the information is not passed. The way actors exchange information is through document provision. In order to disclose some information, an actor would have to provide to others the document(s) containing that information. Hence, to verify if there are any unauthorized disclosures of information, the analysis checks for provisions of documents representing the given information from any unauthorized actors towards other actors.

- **Non\_Modification Violation**

This violation is detected whenever an actor modifies information without having the right to modify it. Non-modification expresses the need that information should not be changed (modified), i.e. authority to modify the information is not granted. To verify if there could be any violations of non-modification, the analysis looks if the authorisee (or an actor that is not authorised by authorised party) modifies the given information. For this, it searches for modify relationships from any goal of this actor to any document representing the given information.

- **Non\_Production Violation**

This violation is detected whenever an actor produces information without having the right to produce it. Non-production expresses the need that information should not be produced in any form, i.e. authority to produce the information is not granted. To verify if there could be any violations of non-production, the analysis checks whether if the authorisee (or an actor that is not authorised by authorised party) produces the given information. For this, it searches for produce relationships from any goal of this actor to any document representing the given information.

- **Non\_Disclosure Violation**

This violation is detected whenever an actor discloses information without having the right to distribute it. Non-disclosure expresses the need of not disclosing or further distributing the given information to other actors, apart from the authoriser. Thus, authority to distribute the information is not passed. The way actors exchange information is through document provision. In order to disclose some information, an actor would have to provide to others the document(s) containing that information. Hence, to verify if there are any unauthorized disclosures of information, the analysis checks for provisions of documents representing the given information from any unauthorized actors towards other actors.

- **NTK Violation**

This violation is detected whenever an actor uses, modifies or produces information for other purposes (goal achievement) than the ones for which it is authorized. Need-to-know requires that the information is used, modified, or produced in the scope of the goals specified in the authorization. This security need concerns confidential information, which should not be utilised for any other purposes other than the intended ones. To verify if there could be any violations of need-to-know, security analysis checks if the authorisee (or an actor that is not authorised by any authorised party) uses, modifies or produces the given information while achieving some goal different from the one it is authorised for. In a nutshell, it searches for need, modify, or produce relationships starting from goals different from the specified ones towards documents representing the given information.

- **Explicit non-reauthorization**

Verifies whether a given actor transfer rights to others even when it does not have the authority to further delegate rights.

- **Non-reauthorization Violation: read**

Verifies whether a given actors transfer to other actors the right to use a given information, without having itself the right to do so.

- **Non-reauthorization Violation: modify**

Verifies whether a given actors transfer to other actors the right to modify a given information, without having itself the right to do so.

- **Non-reauthorization Violation: produce**

Verifies whether a given actors transfer to other actors the right to modify a given information, without having itself the right to do so.

- **Non-reauthorization Violation: transmit**

Verifies whether a given actors transfer to other actors the right to distribute a given information, without having itself the right to do so.

- **SoD Goal Violation**

This violation is detected whenever a single actor may perform both goals, between which an SoD constraint is expressed. Goal-based SoD requires that there is no actor performing both goals among which SoD is specified. To perform this verification, the analysis checks that the final performer of the given goals is not the same actor.

- **BoD Goal Violation**

This violation is detected whenever a single actor may perform both goals, between which an SoD constraint is expressed. Goal-based SoD requires that there is no actor performing both goals among which SoD is specified. To perform this verification, the analysis checks that the final performer of the given goals is not the same actor.

- **Agent Play SoD**

This check verifies the consistency of the Separation of Duty (SoD) constraint between roles. This constraint requires that two roles are not played by the same agent, therefore the check verifies whether there is one agent playing both roles. If that is the case an error is identified, otherwise the check finds no errors.

- **Agent Not Play BoD**

This check verifies the consistency of the Binding of Duty (BoD) constraint between roles. This constraint requires that two roles are played by the same agent, therefore the check verifies whether there is one agent playing both roles. If that is the case the check finds no errors, otherwise an error is identified.

- **Organizational Constraint Consistency**

This check verifies that no conflicting organisational constraints (SoD or BoD) between goals are specified.