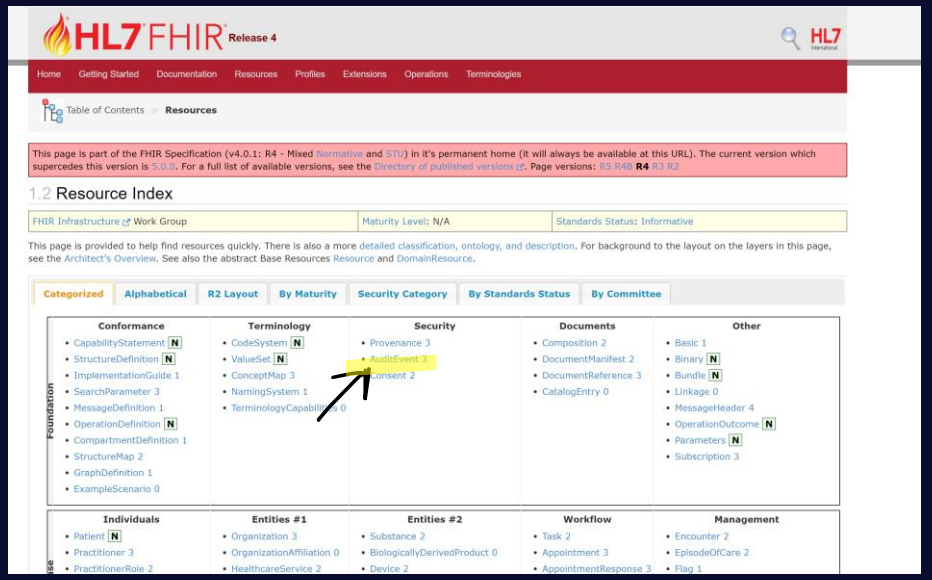
DIPS

ENABLING EFFICIENT HEALTHCARE



Norwegian profiling work on AuditEvent

Trond Elde

Product Leader IAM / 2024-06-12

Leading supplier of e-health solutions

The leading supplier of e-health solutions to Norwegian hospitals

Core business is delivery of patient record systems (EHR) in Norway:

- Prime supplier to 3 out of 4 regional hospital trust – ca. 85 % market share in the specialist health service
- One of the leading suppliers in the municipal health service industry - 155 municipals and ca. 21% market share

Also supplies the market's most complete professional solutions within:

- Health, care, social and child welfare
- LAB, specialist system for diabetes clinics and collaboration solutions for municipalities

Over 300 employees - head office in Bodø, branch offices in Oslo, Bergen, Trondheim, Straume and Tromsø, as well as operations at Sri Lanka

Solid ownership, good financial platform and ambitions for further growth, both national and international

Introduction

- Logging end user (human) activity only - is important to detect information security or privacy breaches in information systems
- Every health care organization has an individual responsibility
- In short: “Who did what, when, from where, for which patient and why?”
  - Login/logout
  - Read document
  - Create a lab requisition
  - Show a list of patients
  - Execute a report
  - Create a referral
  - … etc.
- Compliance requirements in *“Code of conduct for information security and data protection in the healthcare and care services sector”*

Code of conduct requirements

No.	Requirement	Section in the Code	Section in ISO 27001	System requirements in personal health data filing systems for therapeutic purposes	The requirement does not apply in its entirety or in part to the organisation (Must be justified)	Is the requirement fulfilled?	Legal basis for the requirement in law or regulation	The requirement is fulfilled by the processor
200.	Is at least the following logged: • Authorised use of information systems • All system and administrator use for information systems and infrastructure • Configuration and software changes • Security-relevant incidents in security barriers • Attempted unauthorised use of information systems and infrastructure • Use of self-authorisation	5.4.4	A.12.4*	Logging		☐Yes ☐No	PJL, Section 22 HRL, Section 21 GDPR, Section 32 PJF, Section 14	☐Yes ☐No
201.	Is at least the following recorded in the logs in the event of the authorised use of personal health data filing systems for therapeutic purposes: • Identity of the person who retrieved health data • Organisational affiliation of the person who retrieved the health data • The basis for the disclosure • The time period for the disclosure	5.4.4	A.12.4.1 *	Logging		☐Yes ☐No	PJF, Section 14 first paragraph HPL, Section 45 first paragraph	☐Yes ☐No
202.	Are the requirements in the case of the processing of personal health data for purposes other than the provision of healthcare and care services determined on the basis of a risk assessment?	5.4.4	8.2* A.12.4.1 *			☐Yes ☐No	GDPR, Section 32 PJL, Section 22 HRL, Section 21 FLK, Section 7	☐Yes ☐No
203.	Can logs readily be analysed using analysis tools with the aim of detecting breaches?	5.4.4	A.12.4.1 *			☐Yes ☐No	PJF, Section 14 third paragraph	☐Yes ☐No

Source: https://www.ehelse.no/normen/documents-in-english/Appendix%20%E2%80%93%20Overall%20summary%20of%20the%20requirements%20of%20the%20Code.docx

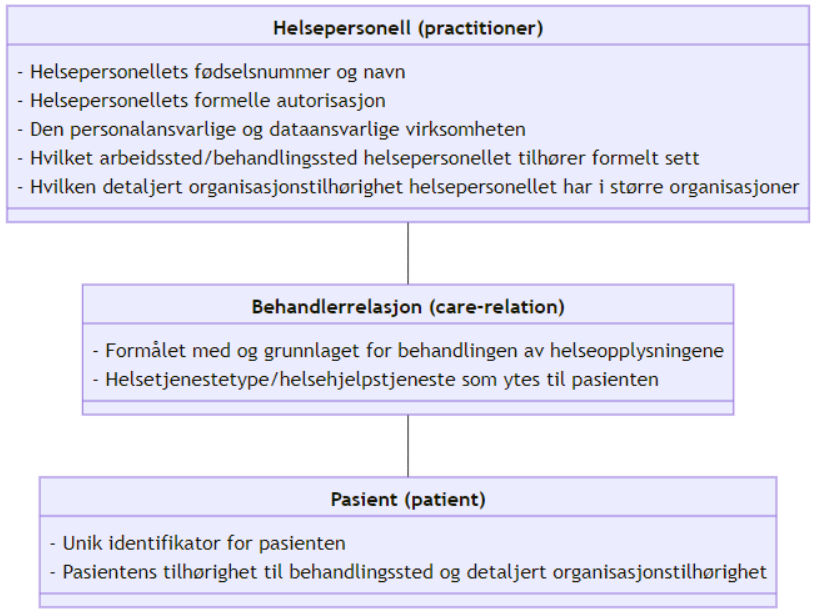
Document/data sharing across organization boundaries

- Trend is more direct API access across health care parties to fulfill the vision of “one resident – one journal” vision in Norway:
  - National services
  - Hospitals
  - Municipal health service
  - GPs (cloud based)

- **Logs from different organizations/systems need to be exposed in a standardized way to be able to do proper analysis for breaches across organization boundaries**

Norwegian Trust Framework (Tillitsrammeverk)

- The Trust Framework provides a specification of a minimum dataset (data model) sharing context specific metadata called *attestation*
- Information model:



Who?

Why?

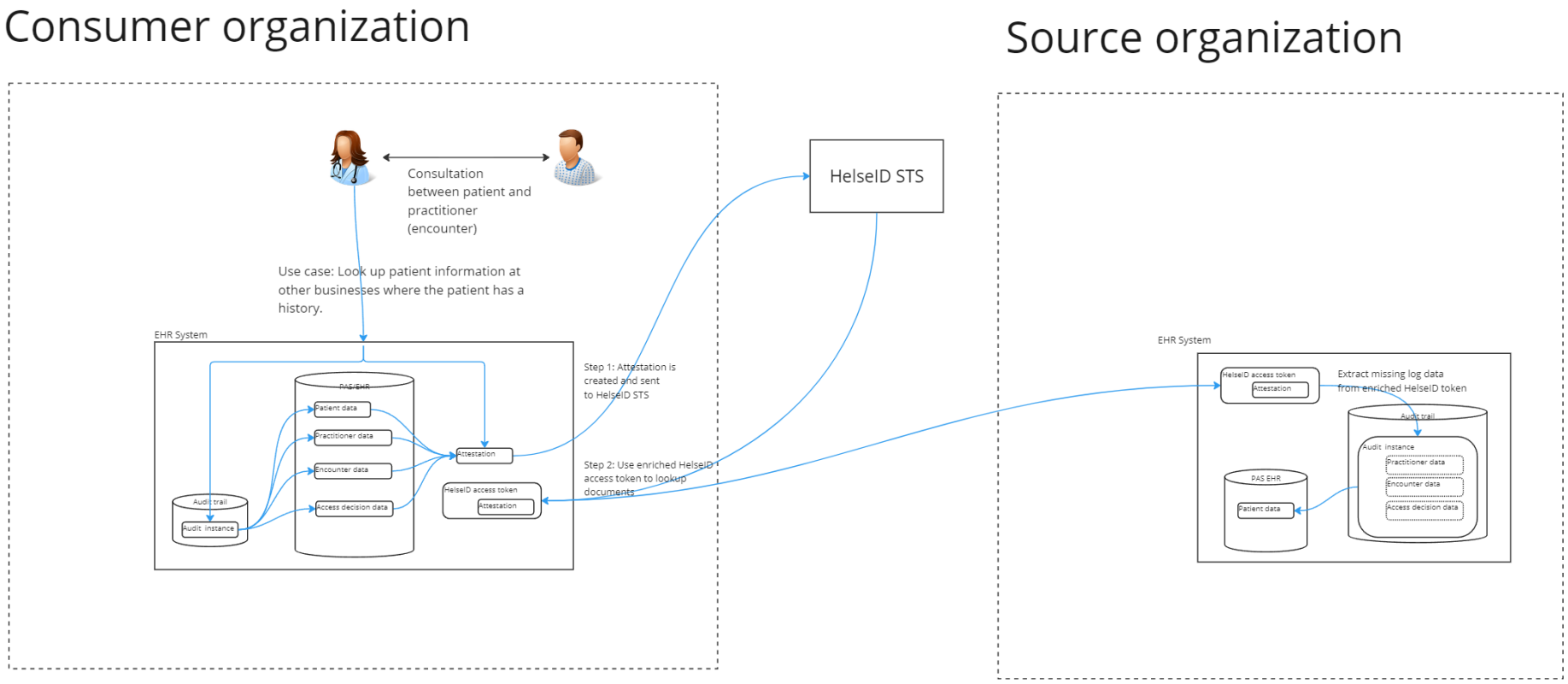
Which patient?

Example of attestation

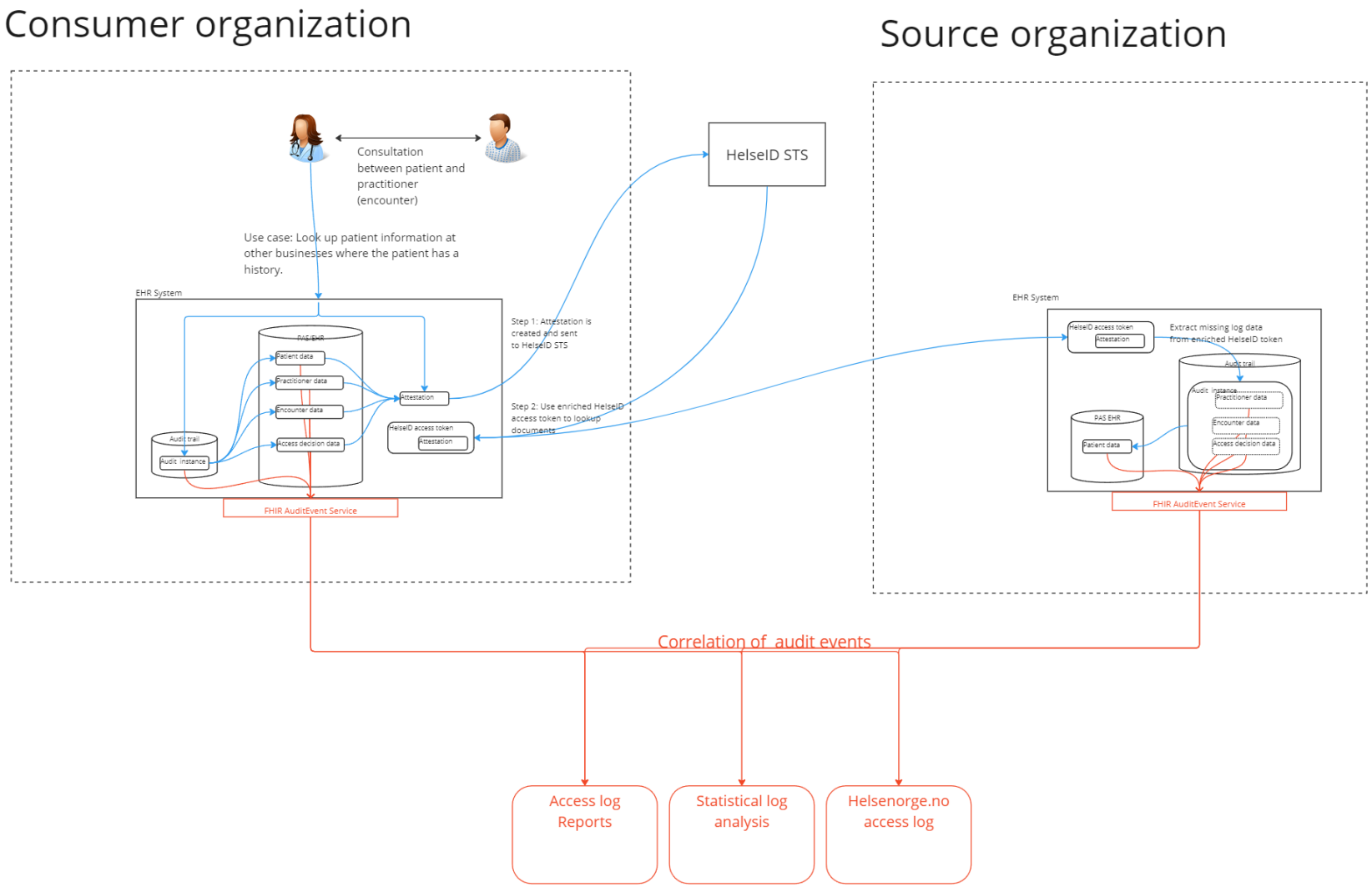

```
{
	"practitioner": {
		"identifier": {
			"id": "05086900124",
			"name": "Ben Reddik",
			"system": "urn:oid:2.16.578.1.12.4.1.4.1",
			"authority": "https://www.skatteetaten.no"
		},
		"hpr_nr": {
			"id": "222200068",
			"system": "urn:oid:2.16.578.1.12.4.1.4.4",
			"authority": "https://www.helsedirektoratet.no/"
		},
		"authorization": {
			"code": "LE",
			"text": "Lege",
			"system": "urn:oid:2.16.578.1.12.4.1.1.9060",
			"assigner": "https://www.helsedirektoratet.no/"
		},
		"legal_entity": {
			"id": "993467049",
			"name": "Oslo universitetssykehus HF",
			"system": "urn:oid:2.16.578.1.12.4.1.4.101",
			"authority": "https://www.brreg.no"
		},
		"point_of_care": {
			"id": "874716782",
			"name": "OSLO UNIVERSITETSSYKEHUS HF RIKSHOSPITALET - SOMATIKK",
			"system": "urn:oid:2.16.578.1.12.4.1.4.101",
			"authority": "https://www.brreg.no"
		},
		"department": {
			"id": "705592",
			"name": "Anestesiologi Seksjon RH",
			"system": "urn:oid:2.16.578.1.12.4.1.4.102",
			"authority": "https://www.nhn.no"
		}
	},
	"care_relation": {
		"healthcare_service": {
			"code": "300",
			"text": "Øyesykdommer",
			"system": "urn:oid:2.16.578.1.12.4.1.1.8451",
			"assigner": "https://www.helsedirektoratet.no/",
		},
		"purpose_of_use": {
			"code": "TREAT",
			"text": "treatment",
			"system": "urn:oid:2.16.840.1.113883.1.11.20448",
			"assigner": "https://www.hl7.org"
		},
		"purpose_of_use_details": {
			"code": "POLBESOK",
			"text": "Poliklinisk besøk",
			"system": "urn:AuditEventHL7Norway/CodeSystem/carerelation",
			"assigner": "https://www.hl7.no"
		}
	},
	"patients": [
		{
			"identifier": {
				"id": "05076600324",
				"system": "urn:oid:2.16.578.1.12.4.1.4.1",
				"authority": "https://www.skatteetaten.no"
			},
			"point_of_care": {
				"id": "974589095",
				"name": "OSLO UNIVERSITETSSYKEHUS HF ULLEVÅL - SOMATIKK",
				"system": "urn:oid:2.16.578.1.12.4.1.4.101",
				"authority": "https://www.brreg.no"
			},
			"department": {
				"id": "109765",
				"name": "Øye dagkir/pol 1. etasje",
				"system": "urn:oid:2.16.578.1.12.4.1.4.102",
				"authority": "https://www.nhn.no"
			}
		}
	]
}
```


[Tillitsrammeverk/specs/informasjons_og_datamodell.md at main · NorskHelsenett/Tillitsrammeverk (github.com)]

Usage of Trust Framework



Exposing audit log data

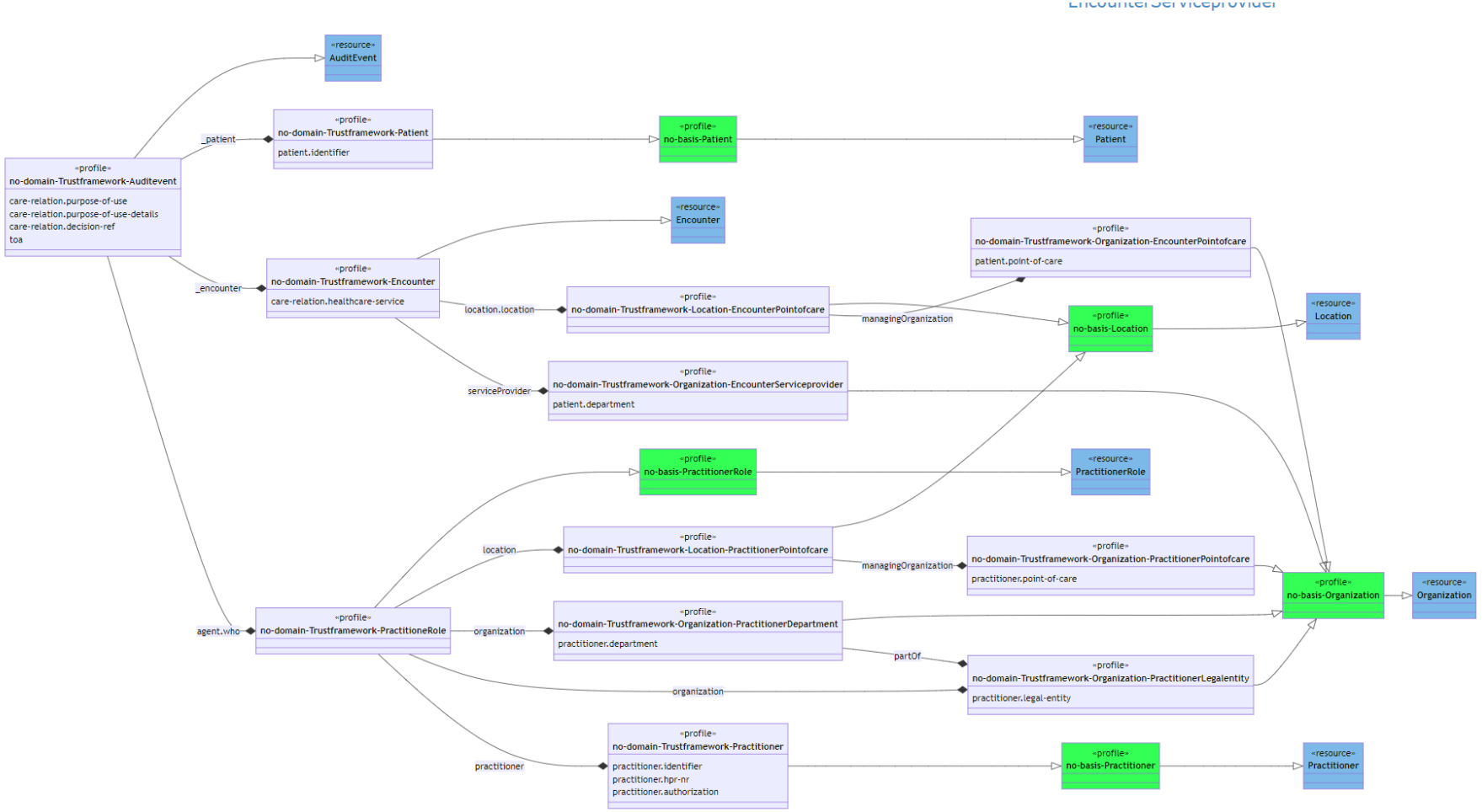


Mapping to FHIR Resources

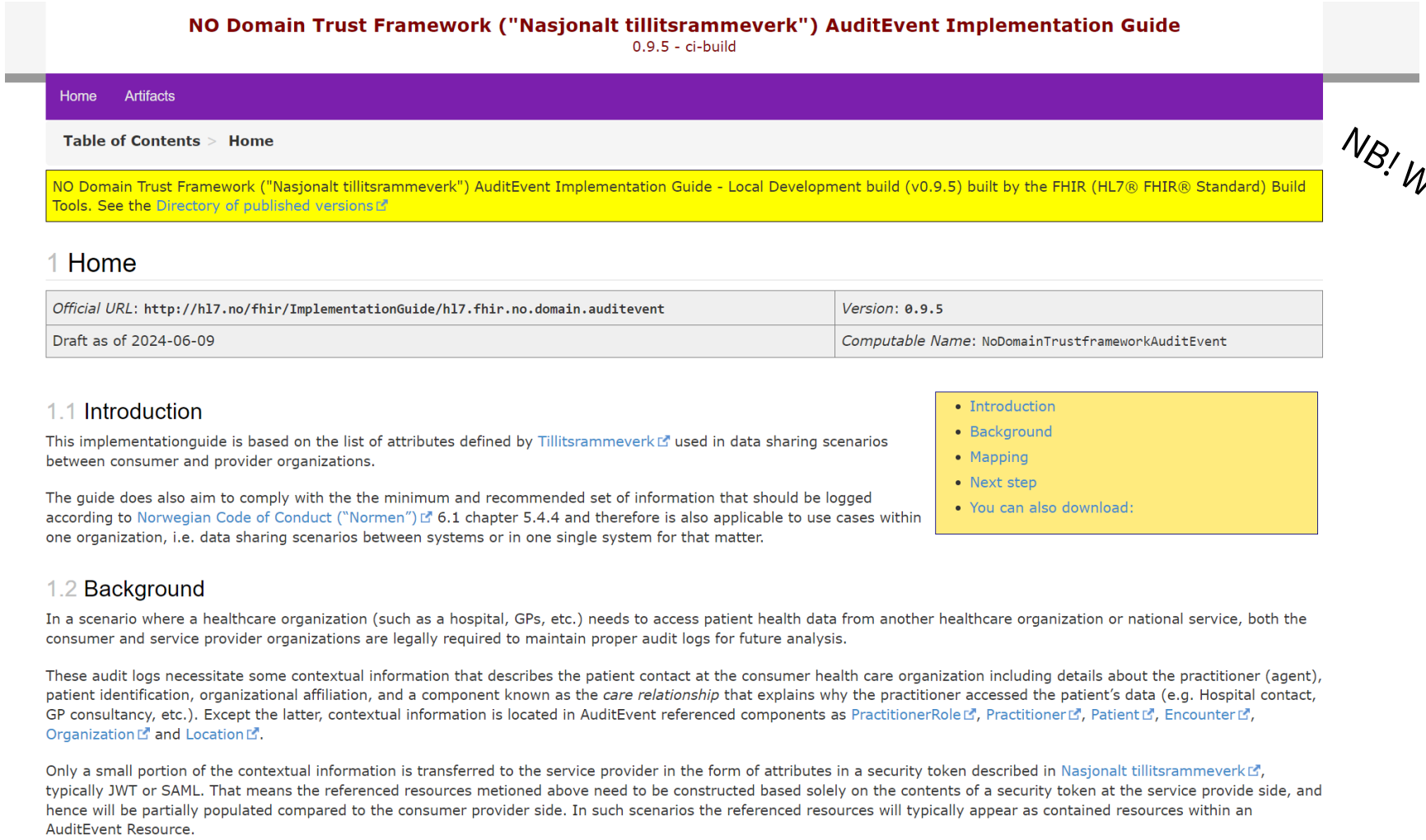
Category	Attribute	Description	Resource
	toa	Time (unix time/epoch time) when the attestation was performed.	AuditEvent
practitioner	identifier	Health personnel's social security number and name from the Norwegian National Registry.	Practitioner
practitioner	hpr-nr	Health personnel's HPR number, if it exists.	Practitioner
practitioner	authorization	Health personnel's authorization, if it exists.	Practitioner
practitioner	legal-entity	The main unit (the legally responsible entity) where the health personnel work, its organization number and name.	Organization
practitioner	point-of-care	The treatment location's organization number and name. It can have the same value as in 'legal-entity'	Organization
practitioner	department	Department/organizational unit where the health personnel provide health care.	Organization
care-relation	healthcare-service	Types of health services provided by the business.	Encounter
care-relation	purpose-of-use	The health personnel's purpose for the health information (what it will be used for).	AuditEvent
care-relation	purpose-of-use-details	Detailed description of the health personnel's purpose for the health information (what it will be used for).	AuditEvent
care-relation	decision-ref	Identification of access decision allowing participant to access patient information.	AuditEvent
patient	identifier	Unique identification of patient	Patient
patient	point-of-care	The business where the patient receives treatment. It can have the same value as in 'legal-entity'.	Organization
patient	department	Department/organizational unit where the patient receives health care.	Organization

DIPS

Creating Trust Framework domain profile structure



Trust Framework ("Nasjonalt tillitsrammeverk") AuditEvent domain profile Implementation Guide



NO Domain Trust Framework ("Nasjonalt tillitsrammeverk") AuditEvent Implementation Guide
0.9.5 - ci-build

Home Artifacts

Table of Contents > Home

NO Domain Trust Framework ("Nasjonalt tillitsrammeverk") AuditEvent Implementation Guide - Local Development build (v0.9.5) built by the FHIR (HL7® FHIR® Standard) Build Tools. See the Directory of published versions

1 Home

Official URL: `http://hl7.no/fhir/ImplementationGuide/hl7.fhir.no.domain.auditevent`	*Version*: `0.9.5`
Draft as of 2024-06-09	*Computable Name*: `NoDomainTrustframeworkAuditEvent`

1.1 Introduction

This implementationguide is based on the list of attributes defined by Tillitsrammeverk used in data sharing scenarios between consumer and provider organizations.

The guide does also aim to comply with the the minimum and recommended set of information that should be logged according to Norwegian Code of Conduct ("Normen") 6.1 chapter 5.4.4 and therefore is also applicable to use cases within one organization, i.e. data sharing scenarios between systems or in one single system for that matter.

- Introduction
- Background
- Mapping
- Next step
- You can also download:

1.2 Background

In a scenario where a healthcare organization (such as a hospital, GPs, etc.) needs to access patient health data from another healthcare organization or national service, both the consumer and service provider organizations are legally required to maintain proper audit logs for future analysis.

These audit logs necessitate some contextual information that describes the patient contact at the consumer health care organization including details about the practitioner (agent), patient identification, organizational affiliation, and a component known as the *care relationship* that explains why the practitioner accessed the patient's data (e.g. Hospital contact, GP consultancy, etc.). Except the latter, contextual information is located in AuditEvent referenced components as PractitionerRole, Practitioner, Patient, Encounter, Organization and Location.

Only a small portion of the contextual information is transferred to the service provider in the form of attributes in a security token described in Nasjonalt tillitsrammeverk, typically JWT or SAML. That means the referenced resources metioned above need to be constructed based solely on the contents of a security token at the service provide side, and hence will be partially populated compared to the consumer provider side. In such scenarios the referenced resources will typically appear as contained resources within an AuditEvent Resource.

NB! Work in progress!

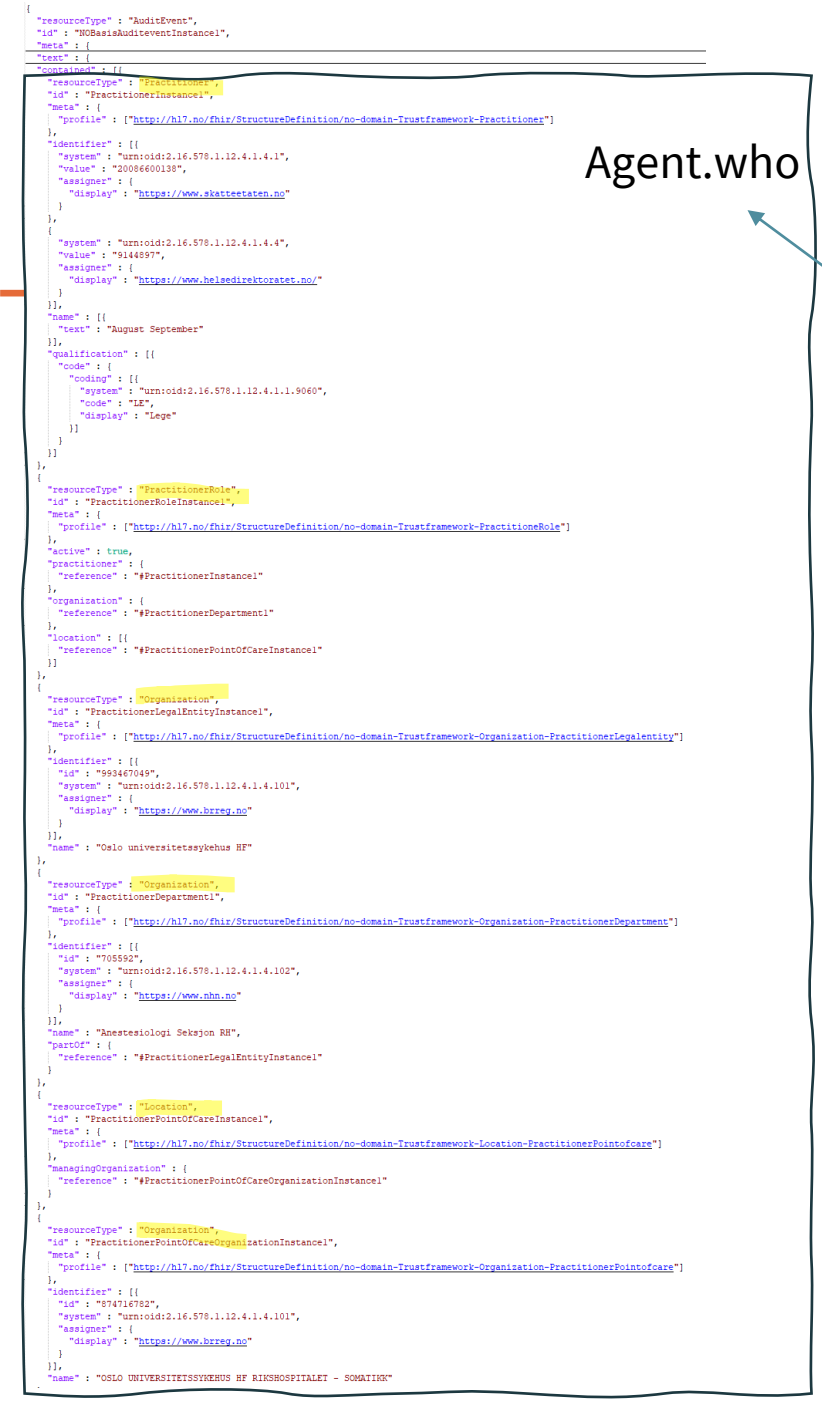
[Home - NO Domain Trust Framework ("Nasjonalt tillitsrammeverk") AuditEvent Implementation Guide v0.9.5 (hl7norway.github.io)]

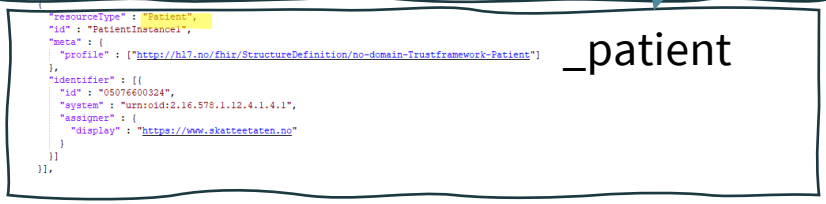
Example of AuditEvent instance with containment

Agent.who

_encounter

_patient





Thank you for your attention

Trond Elde

tre@dips.no

«It’s easy to make it complicated – it’s difficult to make it simple»

DIPS AS
post@dips.no ● dips.no