Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Dipartimento federale dell'interno DFI

RS 816.111

Supplemento 2.2 all'allegato 5 dell'ordinanza del DFI del 22 marzo 2017 sulla cartella informatizzata del paziente

Profili d'integrazione nazionale secondo l'articolo 5 capoverso 1 lettera c OCIP-DFI

Audit Trail Consumption (CH:ATC)

Edizione 2: 24 giugno 2019

Entrate in vigore: 15 luglio 2019

1 Introduction 3
1.1 Definitions of terms 4
1.1.1 EPR circle of trust 4
1.1.2 Patient Identifiers (EPR-SPID, MPI-PID) 4
1.1.3 Terminology 5
2 Volume 1 – Integration Profiles 6
2.1 Overview 6
2.2 Actors, Transactions and Content Modules 7
2.2.1 Actor Descriptions and Actor Profile Requirements 7
2.2.2 Patient Audit Record Repository 7
2.2.3 Patient Audit Consumer 7
2.3 Integration Profile Options 8
2.4 Actor Groupings 8
2.5 Overview – Use Cases 9
2.6 Security Considerations 9
3 Volume 2 – Transactions 9
3.1 Constraints on Retrieve ATNA Audit Event [ITI-81] 9
3.1.1 Message Semantics 9
3.1.2 Additional ATNA Search Parameters 10
3.1.3 Message Semantics for Response 10
3.1.4 Security Considerations 10
3.1.5 Security Audit Considerations 10
4 Volume 3 – Content Profiles 11
4.1 Audit Trail Consumption Event Types 12
4.2 Document Audit Event Content Profile 13
4.2.1 Example Document Audit Event 15
4.3 Policy Audit Event Content Profile 18
4.3.1 Examples 20
4.4 Access Audit Trail Content Profile 24
4.4.1 Example 25
5 Figures 27
6 Tables 27
7 Listings 27

1 Introduction

La cartella informatizzata del paziente (CIP) si basa su un sistema che prevede numerose comunità IHE XDS, in cui il paziente non accorda solo il consenso per la costituzione e l’utilizzo della sua cartella, ma stabilisce esplicitamente anche regole per l'accesso tramite un apposito portale per pazienti.

Il paziente e, se disponibile, il suo rappresentante devono potere consultare i verbali contenuti nella cartella informatizzata presso qualsiasi comunità e comunità di riferimento mediante un apposito portale per pazienti e in una forma leggibile. Questo profilo CH:ATC definisce i requisiti in materia di audit trail consumption che una comunità deve soddisfare in vista dell’audit trail per il paziente.

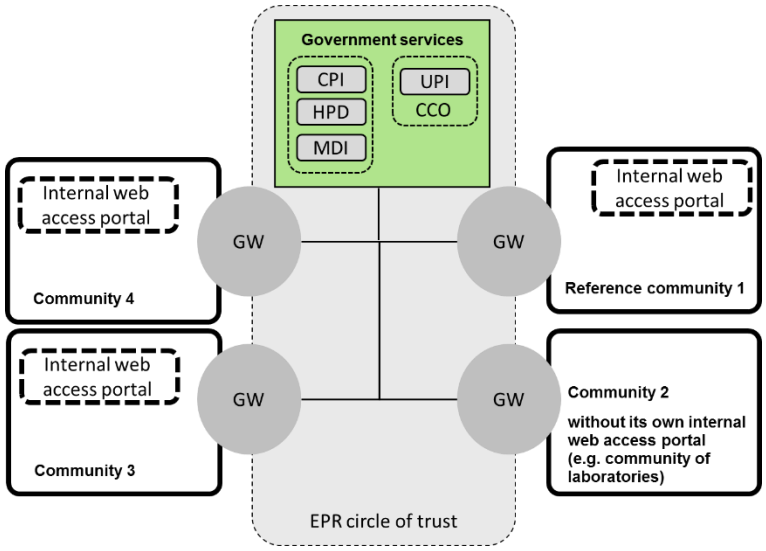
The Swiss Electronic Health Record (EPR) depends on an IHE XDS and multi-community based system where the patient not only consents to the creation and use of the record, but does so by explicitly defining access rules through a patient portal.

Patients – and, if existing, theire representatives – have the right to access the audit trail within the EPR circle of trust. The access to the audit trail will be provided by certified web access portals for patients. This profile CH:ATC defines the audit trail consumption requirements which a community has to meet in order to provide a patients audit trail.

1.1 Definitions of terms

1.1.1 EPR circle of trust

From an organizational perspective and in terms of the Electronic Patient Record Act (EPRA), communities are an association of healthcare professionals and their institutions. Communities who want to participate in the Swiss EPR must comply with the certification requirements as laid down in the implementing provisions for the EPRA. Such communities and, in particular, their gateways will be listed in a community portal index (CPI) provided by the FOPH and therefore form a circle of trust by mutual recognition of their conformity related to data protection and data privacy. Furthermore, all required central services are also part of this circle of trust.



Legend:

GW:	Gateway
CPI:	Community portal Index
HPD:	Healthcare Provider Directory
MDI:	Metadata Index-Service
CCO	Central Compensation Office CCO
UPI:	Unique Person Identification System operated by the CCO

Figure 1: Swiss EPR circle of trust

1.1.2 Patient Identifiers (EPR-SPID, MPI-PID)

Communities in the EPR circle of trust use the national EPR sectoral patient identifier (EPR-SPID) only for cross-community communication. The Federal Central Compensation Office1 (CCO) is the institution which issues EPR-SPID's (EPR Sectorial Personal Identification Number). The CCO is the only institution which is allowed to correlate the Social Security Number (AHVN13) with the EPR-SPID. There is no correlation possible back from the EPR-SPID to the Social Security Number. This is political intention in order to achieve highest possible patient privacy.

Within a community patients are identified by a MPI-PID which is managed by a community Master Patient Index (MPI). Primary Systems may correlate their local patient identifier with the MPI-PID. For cross-community communication the gateways may correlate the MPI-PID to the EPR-SPID.

[1] http://www.zas.admin.ch/index.html

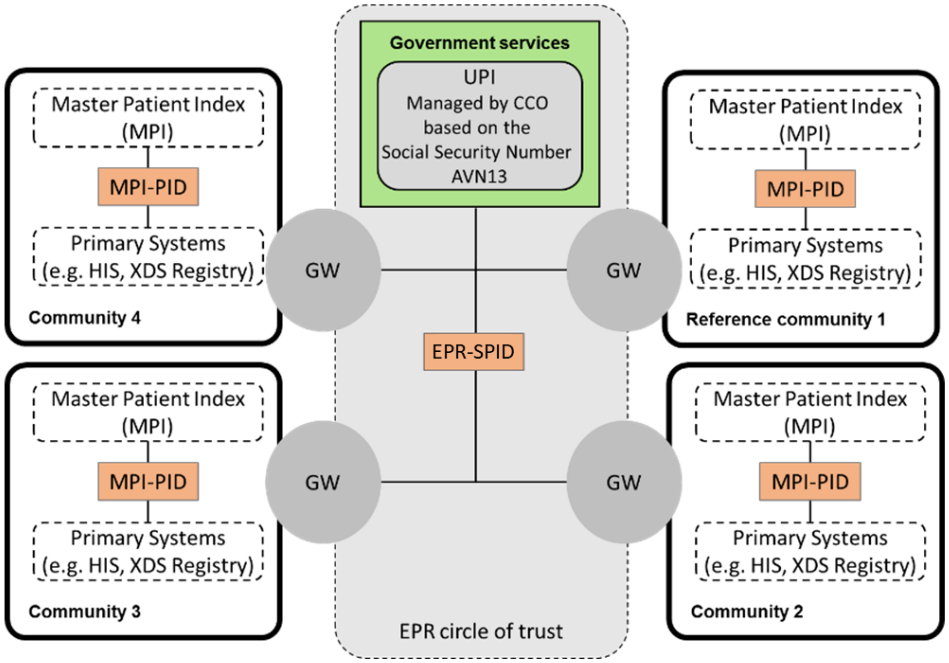


Figure 2: Swiss Patient Identifier

1.1.3 Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119][2].

[2] For full text of RFC2119 see https://www.ietf.org/rfc/rfc2119.txt

2 Volume 1 – Integration Profiles

2.1 Overview

This profile defines the audit trail consumption requirements a community has to provide for a patient's audit trail.

The profile CH:ATC defines and precises the actors and transaction [ITI-81] of the IHE IT Infrastructure Technical Framework Supplement Add RESTful Query to ATNA[3] and defines the content of the Audit Messages. The different types of the Audit Messages are based on the requirements for Document and Policy Access management in order to achieve the Swiss regulation needs on the audit trail access by patients. These Audit Event types differ from the Audit Events which have also to be logged according to the ATNA requirements.

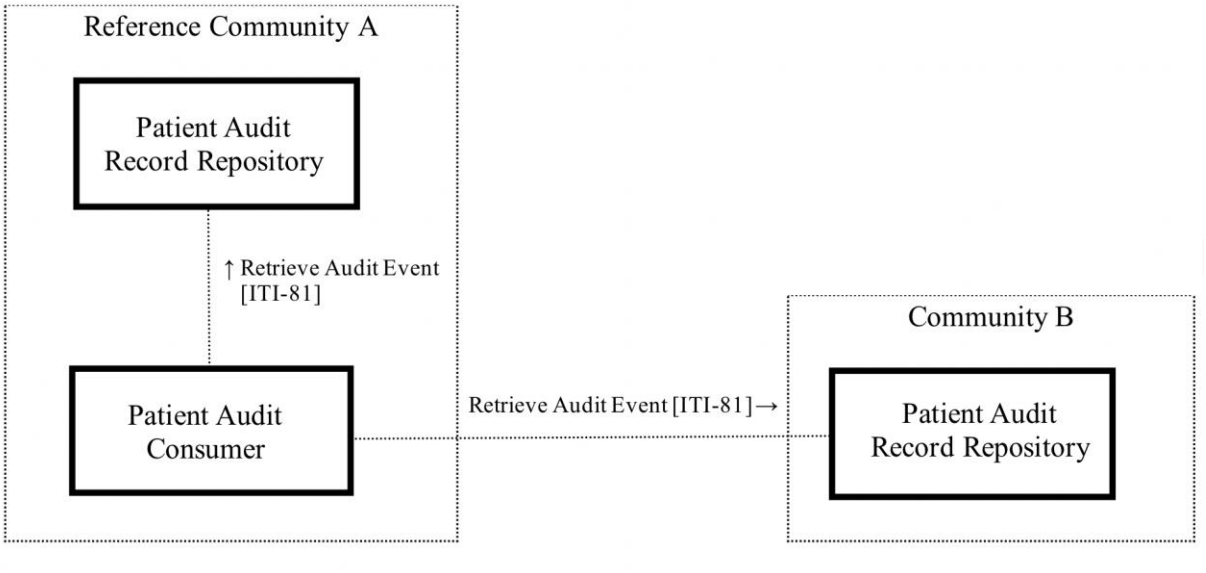


Figure 3: CH:ATC Overview within the Swiss EPR circle of trust

Each community must provide one endpoint to a Patient Audit Record Repository which can be queried according to the [ITI-81] RESTful Query transaction. A reference community must implement a Patient Audit Consumer which will query all Patient Audit Record Repositories, aggregate the results and provide it to the patient.

How the Patient Audit Record Repository generates or collects the specified Document and Policy Access management Audit Events within the community is outside the scope of this profile.

[3] http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_Suppl_RESTful-ATNA.pdf

2.2 Actors, Transactions and Content Modules

Figure 4 shows the actors directly involved in the CH:ATC Profile and the relevant transactions between them. If needed for context, other actors that may be indirectly involved due to their participation in other related profiles are shown in dotted lines.

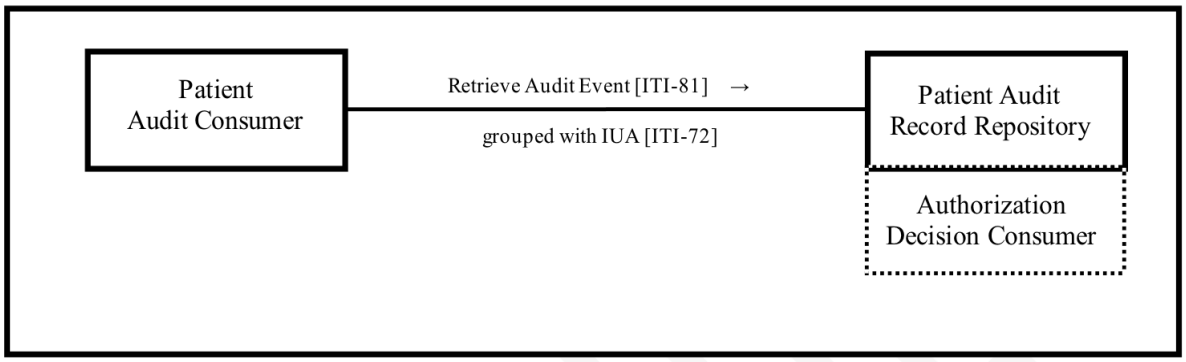


Figure 4: CH:ATC Actor diagram

Table 1 lists the transactions for each actor directly involved in the CH:ATC Profile. To claim compliance with this Profile, an actor shall support all required transactions (labeled "R") and may support the optional transactions (labeled "O").

Actors	Transactions	Initiator or Responder	Opt	Reference
Patient Audit Consumer	Retrieve Audit Event [ITI-81]	Initiator	R	CH:ATC 2.2.3
Patient Audit Record Repository	Retrieve Audit Event [ITI-81]	Responder	R	CH:ATC 2.2.2

Table 1: CH:ATC Profile - Actors and Transactions

2.2.1 Actor Descriptions and Actor Profile Requirements

The actors defined in this profile are based on the IHE IT Infrastructure Technical Framework and the IHE IT Infrastructure Technical Framework Supplement Add RESTful Query to ATNA actors. This section documents any additional requirements on the profile's actors required in the Swiss EPR context.

2.2.2 Patient Audit Record Repository

For the actor Patient Audit Record Repository the actor Audit Record Repository in IHE IT Infrastructure Technical Framework Supplement Add RESTful Query to ATNA is relevant.

The Patient Audit Record Repository shall support the Retrieve Audit Message Option from the Audit Record Repository (ITI TF-1: 9.2.3) with the search capabilities as defined in ITI TF- 2c: 3.81 and the Audit Message Formats defined in Volume 3 – Content Profiles.

2.2.3 Patient Audit Consumer

For the actor Patient Audit Consumer the actor Audit Consumer in IHE IT Infrastructure Technical Framework Supplement Add RESTful Query to ATNA is relevant.

The Patient Audit Consumer queries a Patient Audit Record Repository for Audit Events defined by this profile. The Patient Audit Consumer shall support the Retrieve Audit Message Option from the Audit

Consumer (ITI TF-1: 9.2.3).

The Patient Audit Consumer should filter duplicate AuditEvents for display (e.g. Document Retrieval Audit Event for the same document access are in multiple Patient Audit Record Repositories, because the requesting and responding community need to make the AuditEvent available).

Subsequent processing like translation of the coded elements into the users preferred language and display of the query result is not defined in this profile.

2.3 Integration Profile Options

CH:ATC Actor	Option name
Patient Audit Consumer	Aggregate Audit Message Option
Patient Audit Record Repository	-

Table 2: Actors and Options

The aggregate Audit Message Options allows the Patient Audit Consumer to aggregate results from multiple Patient Audit Record Repositories. A reference community must support at least one Patient Audit Consumer with this Option.

2.4 Actor Groupings

An actor from this profile (Column 1) shall implement all of the required transactions and/or content modules in this profile ***in addition to <u>all</u>*** of the requirements for the grouped actor.

CH:ATC Actor	Grouping Condition	Actor to be grouped with	Reference
Patient Audit Consumer	Required	ATNA - Secure Node	SR 816.11 Amendment 1 of Annex 5
	Required	CT - Time Client	IHE ITI TF Vol 1
	Required	IUA - Authorization Client	IHE ITI Suppl IUA
	Optional	CH:CPI – CPI Consumer	SR 816.11 Amendment 2.3 of Annex 5
Patient Audit Record Repository	Required	ATNA - Secure Node	SR 816.11 Amendment 1 of Annex 5
	Required	CT - Time Client	IHE ITI TF Vol 1
	Required	CH:ADR – Authorization Decision Consumer	SR 816.11 Amendment 2.1 of Annex 5
	Required	IUA - Resource Server	IHE ITI Suppl IUA

Table 3: Actor Grouping

Section 2.6 describes the groupings required for security considerations.

2.5 Overview – Use Cases

Activities related to the EPR are audited for specific document and policy access management events and stored in the communities. This profile supports the following Use Cases:

- A patient can request protocols of the activities related to his EPR.
- A patient representative can request a protocol of the activities related to the patients delegated EPR.

2.6 Security Considerations

The transaction is used to exchange sensitive information and requires authentication and authorization. Grouping of the actors with the ATNA profile is required to ensure TLS Mutual-Authentication, Integrity and Confidentiality.

Access control shall be implemented by grouping the CH:ATC Audit Consumer and Audit Record Repository with the Authorization Client and Resource Server from the IUA trial implementation profile using the SAML Token option (see 3.72.4.1.2.1 in IHE-ITI-Supplement IUA). As defined therein, the CH:ATC Audit Consumer and Audit Record Repository shall implement the ITI-72 Incorporate Authorization Token transaction to convey the XUA token.

The CH:ATC Patient Audit Record Repository shall be grouped with CH:ADR, i.e. the CH:ATC Patient Audit Record Repository shall use the CH:ADR Authorization Decision Request transaction to authorize the transaction and enforce the authorization decision retrieved from CH:ADR Authorization Decision Response.

3 Volume 2 – Transactions

3.1 Constraints on Retrieve ATNA Audit Event [ITI-81]

The Retrieve ATNA Audit Event [ITI-81] transaction is defined in the IHE IT Infrastructure Technical Framework and the IHE IT Infrastructure Technical Framework Supplement Add RESTful Query to ATNA. The following rules shall be applied for the CH:ATC profile.

3.1.1 Message Semantics

The Retrieve ATNA Audit Event message shall be a HTTP GET request sent to the Patient Audit Record Repository. This message is a FHIR search (see http://hl7.org/fhir/STU3/search.html) on AuditEvent Resources (see http://hl7.org/fhir/STU3/auditevent.html). This "search" target is formatted as:

<scheme>://<authority>/<path>/AuditEvent?date=ge[start-time]&date=le[stop- time]&<query>

where:

- **<scheme>** shall be https.
- **<query>** shall include the entity-id as defined in 3.1.2 and may include additional ATNA Search parameters. If entity-id is not included an HTTP response code 400 - Bad Request shall be returned.

3.1.2 Additional ATNA Search Parameters

The Patient Audit Consumer shall not use the following parameters in a query parameters: address, patient.identifier, source, type, user, outcome. The Patient Audit Consumer may use other parameters as listed in [ITI-81].

entity-id is a parameter of token type. This parameter specifies unique identifier for the object. The parameter value should be identified in accordance to the entity type;

For example:

- http://example.com/ARRservice/AuditEvent?date=ge2020-03-22&date=le2025-03-22&entity-id=urn:oid:2.16.756.5.30.1.127.3.10.3|5678

The Audit Record Repository shall match this parameter with the AuditEvent.entity.identifier field that is of type identifier (ParticipantObjectID in DICOM schema).

For the CH:ATC profile the entity-id has to be the EPR-SPID: entity-id=urn:oid:2.16.756.5.30.1.127.3.10.3|<<<value EPR-SPID>>>

3.1.3 Message Semantics for Response

The returned AuditEvent FHIR resources in the Bundle shall conform the CH:ATC AuditEvent profile, see section 4.

3.1.4 Security Considerations

The transaction is used to exchange sensitive information and requires authentication and authorization. Grouping of the actors with the ATNA profile is required to ensure TLS Mutual-Authentication, Integrity and Confidentiality.

Access control shall be implemented by grouping the CH:ATC Audit Consumer and Audit Record Repository with the Authorization Client and Resource Server from the IUA trial implementation profile using the SAML Token option (see 3.72.4.1.2.1 in IHE-ITI-Supplement IUA). As defined therein, the CH:ATC Audit Consumer and Audit Record Repository shall implement the ITI-72 Incorporate Authorization Token transaction to convey the XUA token.

The actors shall implement the ITI-72 transaction with SAML token option, using the base64 encoded SAML assertion defined in XUA to the authorization header of the HTTP1.1 GET request with key IHE-SAML as follows:

GET /example/url/to/resource/location HTTP/1.1
Authorization: IHE-SAML fFBGRNJru1FQd[…omitted for brevity…]44AzqT3Zg
Host: examplehost.com

The CH:ATC Patient Audit Record Repository shall be grouped with CH:ADR, i.e. the CH:ATC Patient Audit Record Repository shall use the CH:ADR Authorization Decision Request transaction to authorize the transaction and enforce the authorization decision retrieved from CH:ADR Authorization Decision Response.

3.1.5 Security Audit Considerations

An audit event as specified in section 4.4 Access Audit Trail Content Profile shall be returned by a query to Patient Audit Record Repository after the Patient Audit Record Repository has been queried by a Patient Audit Consumer.

4 Volume 3 – Content Profiles

Audit Events in the context of the EPR which must be made available for the audit trail fall in three different categories:

- Document management (e.g. a document has been uploaded in the EPR for a patient)
- Policy management (e.g. a patient has given a healthcare professional access rights to his EPR)
- Access Patient Audit Record Repository by a patient or representative (a patient viewed the Audit Trail for the Audit Record Repository)

Each category is described as a content profile. These content profiles are based on the AuditEvent Resource, http://hl7.org/fhir/STU3/auditevent.html.

The AuditEvent Resource has mapping rules to the DICOM audit message format, see FHIR Table 6.4.7.2, http://hl7.org/fhir/STU3/auditevent-mappings.html which allows to map to ATNA.

4.1 Audit Trail Consumption Event Types

The following Audit Trail Consumption Event Types are defined and MUST be supported, see EprAuditTrailConsumptionEventTypes from Codesystem 2.16.756.5.30.1.127.3.10.7.

Type	Description	Profile Ref	Opt Community
ATC_DOC_CREATE	Document upload	4.2	R
ATC_DOC_READ	Document retrieval	4.2	R
ATC_DOC_UPDATE	Document or Document Metadata update	4.2	R
ATC_DOC_DELETE	Document removal	4.2	R
ATC_POL_CREATE_AUT_PART_AL	Authorize participants to access level/date	4.3	R, (NP if not reference community)
ATC_POL_UPDATE_AUT_PART_AL	Update access level/date of authorized participants	4.3	R, (NP: if not reference community)
ATC_POL_REMOVE_AUT_PART_AL	Remove authorization for participants to access level/date	4.3	R, (NP: if not reference community)
ATC_POL_DEF_CONFLEVEL	Set or update the default Confidentiality Level for new documents	4.3	R, (NP: if not reference community)
ATC_POL_DIS_EMER_USE	Disabling Emergency Access	4.3	R, (NP: if not reference community)
ATC_POL_ENA_EMER_USE	Enabling Emergency Access	4.3	R, (NP: if not reference community)
ATC_POL_INCL_BLACKLIST	Assign a Healthcare Professional to Blacklist	4.3	R, (NP: if not reference community)
ATC_POL_EXL_BLACKLIST	Exclude a Healthcare Professional from Blacklist	4.3	R, (NP: if not reference community)
ATC_LOG_READ	Accessing the Patient Audit Record Repository	4.4	R

Table 4: Audit Trail Consumption Event Types

4.2 Document Audit Event Content Profile

This content profile describes Audit Event related to Document Management. The following Data Elements must be provided:

Data Element	Description	Property/Value
Event Type	Document upload Document retrieval Document or Document Metadata update Document removal	
Event Date and Time		UTC
Participants		
Initiator	Patient	Name
	Representative of patient	Name UAP-ID or EPR-SPID
	Authorized Healthcare Professional	Name GLN
	Assistant of a Healthcare Professional	Name GLN
	Technical User	Name Identifier
	Document Administrator	Name UAP-ID
Responsible[4]	Patient	Name
	Healthcare Professional	Name GLN
Groups where Healthcare Professional is member		Name of Group OID
PurposeOfUse		Normal Access, Emergency Access or Automatic Upload
Patient	Involved patient	EPR-SPID
Document	type of document	typeCode[5] (SNOMED CT code)
	reference to document	uniqueId[6] repositoryUniqueId[7] homeCommunityID[8]

Table 5: Document Audit Event Data Elements

[4] If different from Initiator (Representative of patient acting on behalf of a patient then patient is responsible)

[5] SR 816.11, Annex 3, chapter 2.6 type of document (2.16.756.5.30.1.127.3.10.1.27)

[6] IHE TF ITI Vol 3, 4.2.3.2.26 DocumentEntry.uniqueId

[7] IHE TF ITI Vol 3, 4.2.3.2.18 DocumentEntry.repositoryUniqueId

[8] IHE TF ITI Vol 3, 4.2.3.2.12 DocumentEntry.homeCommunityId

This profile defines the content of the document audit events which a community has to provide for a patients audit trail. This profile builds on AuditEvent (http://hl7.org/fhir/STU3/auditevent.html).

Name	Flags	Card.	Type	Description & Constraints
AuditEvent	I	0..*		Document Audit Trail Content Profile **ch-atc-dae-1:** subtype needs to be fixed to ValueSet DocumentAuditEventType
id	Σ	1..1	id	Logical id of this artifact
text		1..1	Narrative	A human-readable narrative that contains the summary of the Audit Event.
type	Σ	1..1	Coding	Type/identifier of event **Binding:** Audit Event ID (extensible)
subtype	Σ		*Coding*	***Slice:*** *Unordered, Open by value:system*
subtype	Σ	1..1	Coding	DocumentAuditEventType **Binding:** DocumentAuditEventType (required)
system		1..1	uri	**Fixed Value:** urn:oid:2.16.756.5.30.1.127.3.10.7
recorded	Σ	1..1	instant	Time when the event was recorded
purposeOfEvent	Σ	1..1	CodeableConcept	The purposeOfUse of the event **Binding:** EprPurposeOfUse (required)
agent		1..*	BackboneElement	Participants
role	Σ	1..1	CodeableConcept	Agent role in the event **Binding:** EprParticipant (required)
userId	Σ	0..1	Identifier	Unique identifier for the user
name	Σ	1..1	string	Human-meaningful name for the agent
requestor	Σ	1..1	boolean	Whether user is initiator
entity	*I*		*BackboneElement*	*Data or objects used* ***Slice:*** *Unordered, Open by value:type.code, value:role.code* ***sev-1:*** *Either a name or a query (NOT both)*
entity	Σ	1..1	BackboneElement	Patient
identifier	Σ	1..1	Identifier	Patient Id (EPR-SPID)
system		1..1	uri	**Fixed Value:** urn:oid:2.16.756.5.30.1.127.3.10.3
type	Σ	1..1	Coding	Type of entity involved
code	Σ	1..1	code	**Fixed Value:** 1
role	Σ	1..1	Coding	What role the entity played
code	Σ	1..1	code	**Fixed Value:** 1
entity	Σ	1..1	BackboneElement	Document
identifier	Σ	1..1	Identifier	XDSDocumentEntry.uniqueId
type	Σ	1..1	Coding	Type of entity involved
code	Σ	1..1	code	**Fixed Value:** 2
role	Σ	1..1	Coding	What role the entity played
code	Σ	1..1	code	**Fixed Value:** 3
detail	*Σ*		*BackboneElement*	***Slice:*** *Unordered, Open by value:type*
detail	Σ	1..1	BackboneElement	repositoryUniqueId
type	Σ	1..1	string	Name of the property **Fixed Value:** Repository Unique Id
value	Σ	1..1	base64Binary	Property value
detail	Σ	1..1	BackboneElement	homeCommunityID
type	Σ	1..1	string	Name of the property **Fixed Value:** homeCommunityID
value	Σ	1..1	base64Binary	Property value
detail	Σ	1..1	BackboneElement	EprDocumentTypeCode
type	Σ	1..1	string	Name of the property **Fixed Value:** EprDocumentTypeCode
value	Σ	1..1	base64Binary	Property value

Table 6: StructureDefinition for Document Audit Event Profile

The mapping from the Document Audit Event Resource to the Data Elements is as follows:

DocumentAuditEvent	CH:ATC Data Element/Property
AuditEvent	
subtype (DocumentAuditEventType)	Event Type
recorded	Event Date and Time
purposeOfEvent	PurposeOfUse
agent	Participants
role	role (PAT, HCP, ASS, REP, TCU, DADM, GRP)
userId	Identifier if applicable
name	Name
requestor	if participant is Initiator
entity	
entity (Patient)	Patient
identifier	EPR-SPID
entity (Document)	Document
identifier	uniqueId
detail (repositoryUniqueId)	repositoryUniqueId
detail (homeCommunityID)	homeCommunityID
detail (EprDocumentTypeCode)	typeCode

Table 7: Mapping Document Audit Event to Data Elements

4.2.1 Example Document Audit Event

Event Resource: type of Document Resource: reference to Document Event Date and Time Participant, Initiator Participant, Responsible	Upload Birth certificate (SOMED CT: 444561001) uniqueID 10.10.2020 18:29 Julia Helfe-Gern representing Jakob Wieder-Gesund

Table 8: Uploading a Birth certificate by a patient representative (atc-doc-create-rep-pat.xml)

```
<AuditEvent xmlns="http://hl7.org/fhir">
  <id value="atc-doc-create-rep-pat"/>
  <meta>
    <profile value="http://fhir.ch/ig/ch-atc/StructureDefinition/DocumentAuditEvent" />
  </meta>
  <text>
    <status value="generated"/>
    <div xmlns="http://www.w3.org/1999/xhtml">Upload of Birth certificate 10.10.2020 18:29 from Julia
Helfe-Gern on behalf of Jakob Wieder-Gesund
  </div>
  </text>
  <type>
    <system value="http://dicom.nema.org/resources/ontology/DCM"/>
    <code value="110106"/>
    <display value="Export"/>
  </type>
```

```
<subtype>
   <system value="urn:oid:2.16.756.5.30.1.127.3.10.7"/>
   <code value="ATC_DOC_CREATE"/>
   <display value="Document upload"/>
</subtype>
<action value="C"/>
<recorded value="2020-10-10T16:29:00Z"/>
<outcome value="0"/>
<purposeOfEvent>
   <coding>
      <system value="urn:oid:2.16.756.5.30.1.127.3.10.5"/>
      <code value="NORM"/>
      <display value="Normal Access"/>
   </coding>
</purposeOfEvent>
<agent>
   <role>
      <coding>
         <system value="urn:oid:2.16.756.5.30.1.127.3.10.6"/>
         <code value="PAT"/>
         <display value="Patient"/>
      </coding>
   </role>
   <name value="Jakob Wieder-Gesund" />
   <requestor value="false" />
</agent>
<agent>
   <role>
      <coding>
         <system value="urn:oid:2.16.756.5.30.1.127.3.10.6"/>
         <code value="REP"/>
         <display value="Representative"/>
      </coding>
   </role>
   <userId>
      <system value="urn:oid:2.16.756.5.30.1.127.3.10.3" />
      <value value="7613222222222222222" />
   </userId>
   <name value="Julia Helfe Gern" />
   <requestor value="true" />
</agent>
<source>
   <identifier>
      <system value="urn:ietf:rfc:3986"/>
      <!-- oid of system generating this audit event -->
      <value value="urn:oid:7.8.9.10.11"/>
   </identifier>
</source>
<entity>
   <!-- Patient -->
   <identifier>
```

```
        <system value="urn:oid:2.16.756.5.30.1.127.3.10.3" />
        <value value="761337610469261945" />
      </identifier>
      <type>
        <system value="http://hl7.org/fhir/audit-entity-type"/>
        <code value="1"/>
        <display value="Person"/>
      </type>
      <role>
        <system value="http://hl7.org/fhir/object-role"/>
        <code value="1"/>
        <display value="Patient"/>
      </role>
    </entity>
    <entity>
      <!-- Document -->
      <identifier>
        <type>
          <coding>
            <system value="urn:uuid:2e82c1f6-a085-4c72-9da3-8640a32e42ab"/>
            <code value="IHE XDS Metadata"/>
            <display value="XDSDocumentEntry.uniqueId"/>
          </coding>
        </type>
        <system value="urn:ietf:rfc:3986"/>
        <value value="urn:oid:1.2.3.4.5"/>
      </identifier>
      <type>
        <system value="http://hl7.org/fhir/audit-entity-type"/>
        <code value="2"/>
        <display value="System Object"/>
      </type>
      <role>
        <system value="http://hl7.org/fhir/object-role"/>
        <code value="3"/>
        <display value="Report"/>
      </role>
      <detail>
        <type value="Repository Unique Id" />
        <value value="MS4yLjM=" />
        <!-- base64 of OID eg 1.2.3 == -->
      </detail>
      <detail>
        <type value="homeCommunityID" />
        <value value="NS42LjcuOA==" />
        <!-- base64 of OID URN homeCommunityId e.g. 5.6.7.8 -->
      </detail>
      <detail>
        <type value="EprDocumentTypeCode" />
        <value value="NDQ0NTYxMDAx" />
        <!-- base64 typeCode 444561001 -->
```

```
      </detail>
   </entity>
</AuditEvent>
```

Listing 1: Example of a document audit event

4.3 Policy Audit Event Content Profile

This content profile describes Audit Events related to Policy Management. The following Data Elements must be provided:

Data Element	Description	Property/Value
Event Type	Authorize participants to access level/date	
	Update access level/date of authorized participants	
	Remove authorization for participants to access level/date	
	Set or update the default Confidentiality Level for new documents	
	Disabling Emergency Access	
	Enabling Emergency Access	
	Assign a Healthcare Professional to Blacklist	
	Exclude a Healthcare Professional from Blacklist	
Event Date Time		UTC
Participants		
Initiator	Patient	Name
	Representative of patient	Name UAP-ID or EPR-SPID
	Authorized Healthcare Professional[9]	Name GLN
	Assistant of a Healthcare Professional[7]	Name GLN
	Policy Administrator	Name UAP-ID
Responsible	Patient	Name
	Healthcare Professional[7]	Name GLN
Patient	Involved patient	EPR-SPID
Resource	Resource Role	HCP, GRP or REP
	Healthcare Professional	Name GLN
	Group of Healthcare Professional	Name of Group OID
	Representative of patient	Name UAP-ID or EPR-SPID

[9] Healthcare Professional or Assistant of Healthcare Professional can only be a participant for the first Event Type (Authorize participants to access level).

	AccessLevel[10]	one of urn:e-health-suisse:2015:policies:access-level: normal, restricted, delegation-and-restricted, delegation-and-normal, full
	AccessLimitedToDate[8]	Date
	ProvideLevel[11]	one of urn:e-health-suisse:2015:policies:provide-level: normal, restricted, secret

Table 9: Policy Audit Event Data Elements

This content profile defines the document audit events which a community has to provide for a patients audit trail. This profile builds on AuditEvent (http://hl7.org/fhir/STU3/auditevent.html).

Name	Flags	Card.	Type	Description & Constraints
AuditEvent	I	0..*		Policy Audit Trail Content Profile **ch-atc-pae-1:** subtype needs to be fixed to ValueSet PolicyAuditEventType
id	Σ	1..1	id	Logical id of this artifact
text		1..1	Narrative	A human-readable narrative that contains the summary of the Audit Event.
type	Σ	1..1	Coding	Type/identifier of event **Binding:** Audit Event ID (extensible)
subtype	Σ		*Coding*	***Slice:*** *Unordered, Open by value:system*
subtype	Σ	1..1	Coding	PolicyAuditEventType **Binding:** PolicyAuditEventType (required)
system		1..1	uri	**Fixed Value:** urn:oid:2.16.756.5.30.1.127.3.10.7
recorded	Σ	1..1	instant	Time when the event was recorded
agent		1..*	BackboneElement	Participants
role	Σ	1..1	CodeableConcept	Agent role in the event **Binding:** EprParticipant (required)
userId	Σ	0..1	Identifier	Unique identifier for the user
name	Σ	1..1	string	Human-meaningful name for the agent
requestor	Σ	1..1	boolean	Whether user is initiator
entity	*I*		*BackboneElement*	*Data or objects used* ***Slice:*** *Unordered, Open by value:type.code* ***sev-1:*** *Either a name or a query (NOT both)*
entity	Σ	1..1	BackboneElement	Patient
identifier	Σ	1..1	Identifier	Patient Id (EPR-SPID)
system		1..1	uri	**Fixed Value:** urn:oid:2.16.756.5.30.1.127.3.10.3
type	Σ	1..1	Coding	Type of entity involved
code	Σ	1..1	code	**Fixed Value:** 1
role	Σ	1..1	Coding	What role the entity played
code	Σ	1..1	code	**Fixed Value:** 1
entity	Σ	0..1	BackboneElement	Resource (HCP, Group, Representative of Patient)
identifier	Σ	0..1	Identifier	Identifier. HCP (GLN), Group (OID)
type	Σ	1..1	Coding	Type of entity involved
code		1..1	code	**Fixed Value:** 2
role	Σ	1..1	Coding	What role the entity played **Binding:** EprParticipant (required)
name	Σ I	1..1	string	Descriptor for entity
detail	*Σ*		*BackboneElement*	***Slice:*** *Unordered, Open by value:type*
detail	Σ	0..1	BackboneElement	AccessLevel if subtype is Create or Update
type	Σ	1..1	string	The type of extra detail provided in the value. **Fixed Value:** AccessLevel
value	Σ	1..1	base64Binary	one of urn:e-health-suisse:2015:policies:access-level: normal,restricted,delegation-and-restricted,delegation-and-normal or full
detail	Σ	0..1	BackboneElement	AccessLimitedToDate if subtype is Create or Update
type	Σ	1..1	string	Name of the property **Fixed Value:** AccessLimitedToDate
value	Σ	1..1	base64Binary	date in Property value
detail	Σ	0..1	BackboneElement	ProvideLevel if subtype is ATC_POL_DEF_CONFLEVEL
type	Σ	1..1	string	Name of the property **Fixed Value:** ProvideLevel
value	Σ	1..1	base64Binary	one of urn:e-health-suisse:2015:policies:provide-level: normal, restricted or secret

Table 10: StructureDefinition for Policy Audit Event Profile

[10] Access Level and the date if the access is limited (AccessLimitedToDate) are required for the first two Event Types (Authorize, update Authorization participants to access level/date) , for the other Event Types these parameters do not need to be specified.

[11] Provide Level is only relevant for the Event Type Default Confidentiality Level for new Documents.

The mapping from the Document Audit Event Resource to the Data Elements is as follows:

PolicyAuditEvent	CH:ATC Data Element/Property
AuditEvent	
subtype (PolicyAuditEventType)	Event Type
recorded	Event Date and Time
agent	Participants
role	role (PAT, HCP, ASS, REP, GRP, PADM)
userId	Identifier if applicable
name	Name
requestor	if participant is Initiator
entity	
entity (Patient)	Patient
identifier	EPR-SPID
entity (Resource)	Resource
identifier	Identifier if applicable
name	Name of HCP, Group or Representative of Patient
detail (AccessLevel)	AccessLevel
detail (AccessLimitedToDate)	AccessLimitedToDate
detail (ProvideLevel)	ProvideLevel

Table 11: Mapping Policy Audit Event to Data Elements

4.3.1 Examples

Event Resource: HCP Event Date and Time Participant Initiator	Create EPR-Access Level "delegation-and-restricted" till 31.12.2020 08:00 to Dr. med. Hans Allzeitbereit 22.09.2020 09:47 Jakob Wieder-Gesund

Table 12: Example Create Delegation and Restricted access for a healthcare professional (atc-pol-create-acc-right.xml)

```
<AuditEvent xmlns="http://hl7.org/fhir">
  <id value="atc-pol-create-acc-right"/>
  <meta>
    <profile value="http://fhir.ch/ig/ch-atc/StructureDefinition/PolicyAuditEvent" />
  </meta>
  <text>
    <status value="generated"/>
    <div xmlns="http://www.w3.org/1999/xhtml">22.09.2020 09:47: Jakob Wieder-Gesund created Ac-
cess Level delegation-and-restricted till 31.12.2020 08:00 to Dr. med. Hans Allzeitbereit
  </div>
  </text>
  <type>
    <system value="http://dicom.nema.org/resources/ontology/DCM"/>
    <code value="110106"/>
```

```
    <display value="Export"/>
  </type>
  <subtype>
    <system value="urn:oid:2.16.756.5.30.1.127.3.10.7"/>
    <code value="ATC_POL_CREATE_AUT_PART_AL"/>
    <display value="Authorize participants to access level/date"/>
  </subtype>
  <action value="C"/>
  <recorded value="2020-10-09T07:47:00Z"/>
  <outcome value="0"/>
  <agent>
    <role>
      <coding>
        <system value="urn:oid:2.16.756.5.30.1.127.3.10.6"/>
        <code value="PAT"/>
        <display value="Patient"/>
      </coding>
    </role>
    <name value="Jakob Wieder-Gesund" />
    <requestor value="true" />
  </agent>
  <source>
    <identifier>
      <system value="urn:ietf:rfc:3986"/>
      <!-- oid of system generating this audit event -->
      <value value="urn:oid:7.8.9.10.12"/>
    </identifier>
  </source>
  <entity>
    <!-- Patient -->
    <identifier>
      <system value="urn:oid:2.16.756.5.30.1.127.3.10.3" />
      <value value="761337610469261945" />
    </identifier>
    <type>
      <system value="http://hl7.org/fhir/audit-entity-type"/>
      <code value="1"/>
      <display value="Person"/>
    </type>
    <role>
      <system value="http://hl7.org/fhir/object-role"/>
      <code value="1"/>
      <display value="Patient"/>
    </role>
  </entity>
  <entity>
    <!-- Resource -->
    <identifier>
      <system value="urn:oid:2.51.1.3" />
      <value value="7601000234438" />
    </identifier>
```

```
      <type>
         <system value="http://hl7.org/fhir/object-type"/>
         <code value="2"/>
         <display value="System Object"/>
      </type>
      <role>
         <system value="urn:oid:2.16.756.5.30.1.127.3.10.6"/>
         <code value="HCP"/>
         <display value="Healthcare professional"/>
      </role>
      <name value="Dr. med. Hans Allzeitbereit" />
      <detail>
         <type value="AccessLevel" />
         <value value="dXJuOmUtaGVhbHRoLXN1aXNzZToyMDE1OnBvbGljaWVzOm-
FjY2Vzcy1sZXZlbDpkZWxlZ2F0aW9uLWFuZC1yZXN0cmljdGVk" />
         <!-- base64 of urn:e-health-suisse:2015:policies:access-level:delegation-and-restricted -->
      </detail>
      <detail>
         <type value="AccessLimitedToDate" />
         <value value="MjAyMC0xMi0zMVQwODowMDowMFo=" />
         <!-- base64 of 2020-12-31-->
      </detail>
   </entity>
</AuditEvent>
```

Listing 2: Example of a create delegation and restricted access for a healthcare professional audit event

Event Resource: Representative Event Date and Time Participant Initiator	Create Julia Helfe Gern 22.09.2020 09:48 Jakob Wieder-Gesund

Table 13: Example Create for a representative (atc-pol-create-acc-right.xml)

```
<AuditEvent xmlns="http://hl7.org/fhir">
   <id value="atc-pol-create-rep"/>
   <meta>
      <profile value="http://fhir.ch/ig/ch-atc/StructureDefinition/PolicyAuditEvent" />
   </meta>
   <text>
      <status value="generated"/>
      <div xmlns="http://www.w3.org/1999/xhtml">22.09.2020 09:48: Jakob Wieder-Gesund authorized
Julia Helfe Gern as a representative
   </div>
   </text>
   <type>
      <system value="http://dicom.nema.org/resources/ontology/DCM"/>
      <code value="110106"/>
      <display value="Export"/>
   </type>
   <subtype>
      <system value="urn:oid:2.16.756.5.30.1.127.3.10.7"/>
```

```
    <code value="ATC_POL_CREATE_AUT_PART_AL"/>
    <display value="Authorize participants to access level/date"/>
  </subtype>
  <action value="C"/>
  <recorded value="2020-10-09T07:48:00Z"/>
  <outcome value="0"/>
  <agent>
    <role>
      <coding>
        <system value="urn:oid:2.16.756.5.30.1.127.3.10.6"/>
        <code value="PAT"/>
        <display value="Patient"/>
      </coding>
    </role>
    <name value="Jakob Wieder-Gesund" />
    <requestor value="true" />
  </agent>
  <source>
    <identifier>
      <system value="urn:ietf:rfc:3986"/>
      <!-- oid of system generating this audit event -->
      <value value="urn:oid:7.8.9.10.12"/>
    </identifier>
  </source>
  <entity>
    <!-- Patient -->
    <identifier>
      <system value="urn:oid:2.16.756.5.30.1.127.3.10.3" />
      <value value="761337610469261945" />
    </identifier>
    <type>
      <system value="http://hl7.org/fhir/audit-entity-type"/>
      <code value="1"/>
      <display value="Person"/>
    </type>
    <role>
      <system value="http://hl7.org/fhir/object-role"/>
      <code value="1"/>
      <display value="Patient"/>
    </role>
  </entity>
  <entity>
    <!-- Resource -->
    <type>
      <system value="http://hl7.org/fhir/object-type"/>
      <code value="2"/>
      <display value="System Object"/>
    </type>
    <role>
      <system value="urn:oid:2.16.756.5.30.1.127.3.10.6"/>
      <code value="REP"/>
```

```
        <display value="Representative"/>
      </role>
      <name value="Julia Helfe Gern" />
   </entity>
</AuditEvent>
```

Listing 3: Example of a create for a representative audit event

4.4 Access Audit Trail Content Profile

This content profile describes Audit Event related to Accessing the Audit Trail of a Patient from a Patient Audit Record Repository. The following Data Elements must be provided:

Data Element	Description	Property/Value
Event Type		Access Audit Trail
Event Date and Time		UTC
Participants		
Initiator	Patient	Name
	Representative of patient	Name UAP-ID or EPR_SPID
Responsible	Patient	Name
Patient	Involved patient	EPR-SPID

Table 14: Access Audit Trail Data Elements

This content profile defines the access audit trail event, which a community has to provide for a patient's audit trail. This profile builds on AuditEvent (http://hl7.org/fhir/STU3/auditevent.html).

Name	Flags	Card.	Type	Description & Constraints
AuditEvent	I	0..*		Access Audit Trail Event Content Profile **ch-atc-aae-1:** subtype needs to be fixed to ATC_LOG_READ
id	Σ	1..1	id	Logical id of this artifact
text		1..1	Narrative	A human-readable narrative that contains the summary of the Audit Event.
type	Σ	1..1	Coding	Type/identifier of event **Binding:** Audit Event ID (extensible)
subtype	Σ	1..1	Coding	**Binding:** AccessAuditTrailEventType (required)
recorded	Σ	1..1	instant	Time when the event was recorded
agent		1..*	BackboneElement	Patient, repeated if representative
role	Σ	1..1	CodeableConcept	Agent role in the event **Binding:** EprParticipant (required)
userId	Σ	0..1	Identifier	Unique identifier for the user
name	Σ	1..1	string	Human-meaningful name for the agent
requestor	Σ	1..1	boolean	Whether user is initiator
entity	*I*		*BackboneElement*	*Data or objects used* ***Slice:** Unordered, Open by value:type.code, value:role.code* ***sev-1:** Either a name or a query (NOT both)*
entity	Σ	1..1	BackboneElement	Patient
identifier	Σ	1..1	Identifier	Patient Id (EPR-SPID)
system		1..1	uri	**Fixed Value:** urn:oid:2.16.756.5.30.1.127.3.10.3
type	Σ	1..1	Coding	Type of entity involved
code	Σ	1..1	code	**Fixed Value:** 1
role	Σ	1..1	Coding	What role the entity played
code	Σ	1..1	code	**Fixed Value:** 1

Table 15: StructureDefinition for Access Audit Trail Event Profile

The mapping from the Access Audit Trail Event Resource to the Data Elements is as follows:

AccessAuditTrailEvent	CH:ATC Data Element/Property
AuditEvent	
subtype (AccessAuditTrailEventType)	Event Type
recorded	Event Date and Time
agent	Participants
role	role (PAT, REP)
userId	Identifier if applicable
name	Name
requestor	if participant is Initiator
entity	
entity (Patient)	Patient
identifier	EPR-SPID

Table 16: Mapping Access Audit Trail Event to Data Elements

4.4.1 Example

Event Patient Timestamp Participant	Access Audit Trail Jakob Wieder-Gesund 22.09.2020 10:47 Jakob Wieder-Gesund

Table 17: Example Log Access (atc-log-read.xml)

```
<AuditEvent xmlns="http://hl7.org/fhir">
   <id value="atc-log-read"/>
   <meta>
      <profile value="http://fhir.ch/ig/ch-atc/StructureDefinition/AccessAuditTrailEvent" />
   </meta>
   <text>
      <status value="generated"/>
      <div xmlns="http://www.w3.org/1999/xhtml">Jakob Wieder-Gesund has viewed the audit trail
22.09.2020 10:47
 </div>
   </text>
   <type>
      <system value="http://dicom.nema.org/resources/ontology/DCM"/>
      <code value="110106"/>
      <display value="Export"/>
   </type>
   <subtype>
      <system value="urn:oid:2.16.756.5.30.1.127.3.10.7"/>
      <code value="ATC_LOG_READ"/>
      <display value="Accessing the Patient Audit Record Repository"/>
```

```
  </subtype>
  <action value="C"/>
  <recorded value="2020-09-22T08:47:00Z"/>
  <outcome value="0"/>
  <agent>
    <role>
      <coding>
        <system value="urn:oid:2.16.756.5.30.1.127.3.10.6"/>
        <code value="PAT"/>
        <display value="Patient"/>
      </coding>
    </role>
    <name value="Jakob Wieder-Gesund" />
    <requestor value="true" />
  </agent>
  <source>
    <identifier>
      <system value="urn:ietf:rfc:3986"/>
      <!-- oid of system generating this audit event -->
      <value value="urn:oid:7.8.9.10.11"/>
    </identifier>
  </source>
  <entity>
    <!-- Patient -->
    <identifier>
      <system value="urn:oid:2.16.756.5.30.1.127.3.10.3" />
      <value value="761337610469261945" />
    </identifier>
    <type>
      <system value="http://hl7.org/fhir/audit-entity-type"/>
      <code value="1"/>
      <display value="Person"/>
    </type>
    <role>
      <system value="http://hl7.org/fhir/object-role"/>
      <code value="1"/>
      <display value="Patient"/>
    </role>
  </entity>
</AuditEvent>
```

Listing 4: Example of a log access audit event

5 Figures

Figure 1: Swiss EPR circle of trust 4
Figure 2: Swiss Patient Identifier 5
Figure 3: CH:ATC Overview within the Swiss EPR circle of trust 6
Figure 4: CH:ATC Actor diagram 7

6 Tables

Table 1: CH:ATC Profile - Actors and Transactions 7
Table 2: Actors and Options 8
Table 3: Actor Grouping 8
Table 4: Audit Trail Consumption Event Types 12
Table 5: Document Audit Event Data Elements 13
Table 6: StructureDefinition for Document Audit Event Profile 14
Table 7: Mapping Document Audit Event to Data Elements 15
Table 8: Uploading a Birth certificate by a patient representative (atc-doc-create-rep-pat.xml) 15
Table 9: Policy Audit Event Data Elements 19
Table 10: StructureDefinition for Policy Audit Event Profile 19
Table 11: Mapping Policy Audit Event to Data Elements 20
Table 12: Example Create Delegation and Restricted access for a healthcare professional (atc-pol-create-acc-right.xml) 20
Table 13: Example Create for a representative (atc-pol-create-acc-right.xml) 22
Table 14: Access Audit Trail Data Elements 24
Table 15: StructureDefinition for Access Audit Trail Event Profile 24
Table 16: Mapping Access Audit Trail Event to Data Elements 25
Table 17: Example Log Access (atc-log-read.xml) 25

7 Listings

Listing 1: Example of a document audit event 18
Listing 2: Example of a create delegation and restricted access for a healthcare professional audit event 22
Listing 3: Example of a create for a representative audit event 24
Listing 4: Example of a log access audit event 26