SR 816.111
Ergänzung 2.2 zu Anhang 5 der Verordnung des EDI vom 22. März 2017 über das elektronische Patienten­dossier

Nationale Integrationsprofile nach Artikel 5 Absatz 1 Buchstabe c EPDV-EDI

Audit Trail Consumption (CH:ATC)

Ausgabe 2: 24. Juni 2019
Inkrafttreten: 15. Juli 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

Das elektronische Patientendossier (EPD) basiert auf einem System mit mehreren IHE XDS-Gemeinschaften, in welchem die Patientin oder der Patient nicht nur die Zustimmung zur Erstellung und Verwendung ihres oder seines Dossiers gibt, sondern auch explizit Zugangsregeln durch ein Zugangsportal für Patientinnen und Patienten festlegt.

Patientinnen und Patienten – und, falls vorhanden, deren Stellvertretung – müssen die Möglichkeit haben, die Protokolldaten zu ihrem elektronischen Patientendossier aus allen Gemeinschaften und Stammgemeinschaften in einer für sie lesbaren Form im Patientenportal der Stammgemeinschaft einsehen. Dieses Profil CH:ATC definiert die Audit-Trail-Consumption Anforderungen, die eine Gemeinschaft für das Bereitstellen des Patienten-Audit-Trail erfüllen muss.

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, their 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.

![Swiss EPR circle of trust](http://www.zas.admin.ch/index.html)

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

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
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 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 precis the actors and transaction [ITI-81] of the IHE IT Infrastructure Technical Framework Supplement Add RESTful Query to ATNA³ 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.

![Diagram of CH:ATC Overview within the Swiss EPR circle of trust](http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_Suppl_RESTful-ATNA.pdf)

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 [Link to IHE IT Infrastructure Technical Framework Supplement Add RESTful Query to ATNA](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.

![CH:ATC Actor diagram](image)

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”).

<table>
<thead>
<tr>
<th>Actors</th>
<th>Transactions</th>
<th>Initiator or Responder</th>
<th>Opt</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Patient Audit Consumer</td>
<td>Retrieve Audit Event [ITI-81]</td>
<td>Initiator</td>
<td>R</td>
<td>CH:ATC 2.2.3</td>
</tr>
<tr>
<td>Patient Audit Record Repository</td>
<td>Retrieve Audit Event [ITI-81]</td>
<td>Responder</td>
<td>R</td>
<td>CH:ATC 2.2.2</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>CH:ATC Actor</th>
<th>Option name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Patient Audit Consumer</td>
<td>Aggregate Audit Message Option</td>
</tr>
<tr>
<td>Patient Audit Record Repository</td>
<td>-</td>
</tr>
</tbody>
</table>

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 all 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                     |                                               |
| 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](http://hl7.org/fhir/STU3/search.html)) on AuditEvent Resources (see [http://hl7.org/fhir/STU3/auditevent.html](http://hl7.org/fhir/STU3/auditevent.html)). This “search” target is formatted as:

```xml
<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 IFBGRNJru1FQd[...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](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](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.

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

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:

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

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).

Table 6: StructureDefinition for Document Audit Event Profile
The mapping from the Document Audit Event Resource to the Data Elements is as follows:

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

Table 7: Mapping Document Audit Event to Data Elements

4.2.1 Example Document Audit Event

<table>
<thead>
<tr>
<th>Event</th>
<th>Upload</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resource: type of Document</td>
<td>Birth certificate (SOMED CT: 444561001)</td>
</tr>
<tr>
<td>Resource: reference to Document</td>
<td>uniqueID</td>
</tr>
<tr>
<td>Event Date and Time</td>
<td>10.10.2020 18:29</td>
</tr>
<tr>
<td>Participant, Initiator</td>
<td>Julia Helfe-Gern</td>
</tr>
<tr>
<td>Participant, Responsible</td>
<td>representing Jakob Wieder-Gesund</td>
</tr>
</tbody>
</table>

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

```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>
</AuditEvent>
Ergänzung 2.2 zu Anhang 5 der EPDV-EDI: Nationale Integrationsprofile

<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="761322222222222222"/>
  </userId>
  <name value="Julia Helfe Gern"/>
  <requestor value="true"/>
</agent>
<source>
  <identifier>
    <system value="urn:ietf:rfc:3986"/>
  </identifier>
</source>
<entity>
  <!-- Patient -->
</entity>
Ergänzung 2.2 zu Anhang 5 der EPDV-EDI: Nationale Integrationsprofile

<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="NS42LjcuaO=" />
<!-- base64 of OID URN homeCommunityId e.g. 5.6.7.8 -->
</detail>
<detail>
<type value="EprDocumentTypeCode" />
<value value="NDQ0NTYxMDAx" />
<!-- base64 typeCode 444561001 -->
</detail>
### 4.3 Policy Audit Event Content Profile

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

<table>
<thead>
<tr>
<th>Data Element</th>
<th>Description</th>
<th>Property/Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Event Type</strong></td>
<td>Authorize participants to access level/date</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Update access level/date of authorized participants</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Remove authorization for participants to access level/date</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Set or update the default Confidentiality Level for new documents</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Disabling Emergency Access</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Enabling Emergency Access</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Assign a Healthcare Professional to Blacklist</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Exclude a Healthcare Professional from Blacklist</td>
<td></td>
</tr>
<tr>
<td><strong>Event Date Time</strong></td>
<td>Event Date Time</td>
<td>UTC</td>
</tr>
<tr>
<td><strong>Participants</strong></td>
<td>Initiator</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Patient</td>
<td>Name</td>
</tr>
<tr>
<td></td>
<td>Representative of patient</td>
<td>Name</td>
</tr>
<tr>
<td></td>
<td>Authorized Healthcare Professional</td>
<td>Name</td>
</tr>
<tr>
<td></td>
<td>Assistant of a Healthcare Professional</td>
<td>Name</td>
</tr>
<tr>
<td></td>
<td>Policy Administrator</td>
<td>Name</td>
</tr>
<tr>
<td><strong>Responsible</strong></td>
<td>Patient</td>
<td>Name</td>
</tr>
<tr>
<td></td>
<td>Healthcare Professional</td>
<td>Name</td>
</tr>
<tr>
<td><strong>Patient</strong></td>
<td>Involved patient</td>
<td>EPR-SPID</td>
</tr>
<tr>
<td><strong>Resource</strong></td>
<td>Resource Role</td>
<td>HCP, GRP or REP</td>
</tr>
<tr>
<td></td>
<td>Healthcare Professional</td>
<td>Name</td>
</tr>
<tr>
<td></td>
<td>Group of Healthcare Professional</td>
<td>Name of Group</td>
</tr>
<tr>
<td></td>
<td>Representative of patient</td>
<td>Name</td>
</tr>
</tbody>
</table>

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

### Table 9: Policy Audit Event Data Elements

<table>
<thead>
<tr>
<th>Name</th>
<th>Flags</th>
<th>Card.</th>
<th>Type</th>
<th>Description &amp; Constraints</th>
</tr>
</thead>
<tbody>
<tr>
<td>AuditEvent</td>
<td>1</td>
<td>C</td>
<td>Policy Audit Trail Contains Profile</td>
<td></td>
</tr>
<tr>
<td>id</td>
<td>2</td>
<td>1.1</td>
<td>ID</td>
<td>Unique identifier of the event.</td>
</tr>
<tr>
<td>text</td>
<td>3</td>
<td>1.1</td>
<td>Narrative</td>
<td>A human-readable narrative that contains the summary of the Audit Event.</td>
</tr>
<tr>
<td>type</td>
<td>3</td>
<td>1.1</td>
<td>Coding</td>
<td>Type of the event.</td>
</tr>
<tr>
<td>subtype</td>
<td>2</td>
<td>1.1</td>
<td>Coding</td>
<td>Either an identifier or a profile.</td>
</tr>
<tr>
<td>system</td>
<td>3</td>
<td>1.1</td>
<td>url</td>
<td>A resource identifier or a computer readable name that identifies the resource.</td>
</tr>
<tr>
<td>recorded</td>
<td>2</td>
<td>1.1</td>
<td>boolean</td>
<td>Indicates whether the event is recorded.</td>
</tr>
<tr>
<td>agent</td>
<td></td>
<td>1</td>
<td>BackboneElement</td>
<td>The agent is an entity that is related to the event.</td>
</tr>
<tr>
<td>role</td>
<td>2</td>
<td>1.1</td>
<td>CodeableConcept</td>
<td>Role of the participant.</td>
</tr>
<tr>
<td>user/identifier</td>
<td>3</td>
<td>0.1</td>
<td>Identifier</td>
<td>Unique identifier for the user.</td>
</tr>
<tr>
<td>name</td>
<td>2</td>
<td>1.1</td>
<td>string</td>
<td>Human-meaningful name for the agent.</td>
</tr>
<tr>
<td>user/oressor</td>
<td>3</td>
<td>0.1</td>
<td>boolean</td>
<td>Whether user is visitor.</td>
</tr>
<tr>
<td>date</td>
<td>1</td>
<td>1.1</td>
<td>Coding</td>
<td>Date of the event.</td>
</tr>
<tr>
<td>code</td>
<td>3</td>
<td>1.1</td>
<td>code</td>
<td>Code of the event.</td>
</tr>
<tr>
<td>rate</td>
<td>3</td>
<td>1.1</td>
<td>Coding</td>
<td>Rate of the event.</td>
</tr>
<tr>
<td>reason</td>
<td>1</td>
<td>1.1</td>
<td>Coding</td>
<td>Reason for the event.</td>
</tr>
<tr>
<td>entity</td>
<td>2</td>
<td>1.1</td>
<td>BackboneElement</td>
<td>The entity is an entity that is related to the event.</td>
</tr>
<tr>
<td>identifier</td>
<td>2</td>
<td>1.1</td>
<td>Identifier</td>
<td>Identifiers that identify the entity.</td>
</tr>
<tr>
<td>name</td>
<td>3</td>
<td>1.1</td>
<td>string</td>
<td>Name of the entity.</td>
</tr>
<tr>
<td>detail</td>
<td>2</td>
<td>1.1</td>
<td>BackboneElement</td>
<td>Details about the event.</td>
</tr>
<tr>
<td>type</td>
<td>1</td>
<td>1</td>
<td>string</td>
<td>The type of the detail.</td>
</tr>
<tr>
<td>value</td>
<td>2</td>
<td>1.1</td>
<td>string</td>
<td>The value of the detail.</td>
</tr>
</tbody>
</table>

### Table 10: StructureDefinition for Policy Audit Event Profile

<table>
<thead>
<tr>
<th>Name</th>
<th>Flags</th>
<th>Card.</th>
<th>Type</th>
<th>Description &amp; Constraints</th>
</tr>
</thead>
<tbody>
<tr>
<td>AccessLimitedToDate8</td>
<td></td>
<td></td>
<td>Date</td>
<td></td>
</tr>
<tr>
<td>ProvideLevel11</td>
<td></td>
<td></td>
<td>one of urn:e-health-suisse:2015:policies:provide-level: normal, restricted, secret</td>
<td></td>
</tr>
</tbody>
</table>

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:

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

Table 11: Mapping Policy Audit Event to Data Elements

### 4.3.1 Examples

<table>
<thead>
<tr>
<th>Event Resource: HCP</th>
<th>Create</th>
</tr>
</thead>
<tbody>
<tr>
<td>Event Date and Time</td>
<td>EPR-Access Level &quot;delegation-and-restricted&quot;</td>
</tr>
<tr>
<td>Participant Initiator</td>
<td>till 31.12.2020 08:00 to Dr. med. Hans Alzeitbereit</td>
</tr>
<tr>
<td></td>
<td>22.09.2020 09:47 Jakob Wieder-Gesund</td>
</tr>
</tbody>
</table>

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

```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"/>
  </text>
  <type>
    <system value="http://dicom.nema.org/resources/ontology/DCM"/>
    <code value="110106"/>
  </type>
</AuditEvent>
```
Listing 2: Beispiel einer Delegation und verringerten Zugriff für eine Gesundheitsberufe-Audit-Event

<table>
<thead>
<tr>
<th>Event</th>
<th>Create</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resource: Representative</td>
<td>Julia Helfe Gern</td>
</tr>
<tr>
<td>Event Date and Time</td>
<td>22.09.2020 09:48</td>
</tr>
<tr>
<td>Participant Initiator</td>
<td>Jakob Wieder-Gesund</td>
</tr>
</tbody>
</table>

Tabelle 13: Beispiel Erstellen für einen Vertreter (atc-pol-create-acc-right.xml)
<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>
</entity>
<entity>
  <!-- Resource -->
  <type>
    <system value="http://hl7.org/fhir/audit-entity-type"/>
    <code value="1"/>
    <display value="Person"/>
  </type>
</entity>
<entity>
  <type>
    <system value="http://hl7.org/fhir/object-role"/>
    <code value="1"/>
    <display value="Patient"/>
  </type>
</entity>
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:

<table>
<thead>
<tr>
<th>Data Element</th>
<th>Description</th>
<th>Property/Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Event Type</td>
<td>Access Audit Trail</td>
<td></td>
</tr>
<tr>
<td>Event Date and Time</td>
<td>UTC</td>
<td></td>
</tr>
<tr>
<td>Participants</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Initiator</td>
<td>Patient</td>
<td>Name</td>
</tr>
<tr>
<td></td>
<td>Representative of patient</td>
<td>Name</td>
</tr>
<tr>
<td>Responsible</td>
<td>Patient</td>
<td>Name</td>
</tr>
<tr>
<td>Patient</td>
<td>Involved patient</td>
<td>EPR-SPID</td>
</tr>
</tbody>
</table>

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).

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:

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

Table 16: Mapping Access Audit Trail Event to Data Elements

4.4.1 Example

<table>
<thead>
<tr>
<th>Event</th>
<th>Access Audit Trail Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>Patient</td>
<td>Jakob Wieder-Gesund</td>
</tr>
<tr>
<td>Timestamp</td>
<td>22.09.2020 10:47</td>
</tr>
<tr>
<td>Participant</td>
<td>Jakob Wieder-Gesund</td>
</tr>
</tbody>
</table>

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

```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>
    <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>
</AuditEvent>
```
Listing 4: Example of a log access audit event

```xml
<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>
```
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