Nationwide Health Information Network (NHIN)

Trial Implementations

Service Interface Specifications

Audit Log Query

V 1.3.1

01/30/2009

Contributors

Name	Organization	NHIE represented
Taha Abdul-Basser	Wellogic	NCHICA, MedVA
David Riley	FHA	Federal NHIE

Document Change History

Version	Date	Changed By	Items Changed Since Previous Version
1.0	6/5/2008	Taha Abdul-Basser	Initial Draft
1.3.1	01/30/2009	David L. Riley	Format/edit changes to prepare for publication

Document Approval

Version	Date	Approved By	Role
1.0		NHIN Cooperative Technical and Security Working Group	

Table of Contents

1 Preface

1.1 Introduction

The NHIN Trial Implementations Service Interface Specifications constitute the core services of an operational Nationwide Health Information Network. They are intended to provide a standard set of service interfaces that enable Nationwide Health Information Exchange (NHIE) to NHIE exchange of interoperable health information. These services provide such functional capabilities as patient look-up, document query and retrieve, notification of consumer preferences, and access to logs for determining who has accessed what records and for what purpose for use. These functional services rest on a foundational set of messaging and security services. The current set of defined core services includes the following:

1. NHIN Trial Implementations Message Platform Service Interface Specification,
2. NHIN Trial Implementations Authorization Framework Service Interface Specification,
3. NHIN Trial Implementations Subject Discovery Service Interface Specification,
4. NHIN Trial Implementations Query for Documents Service Interface Specification,
5. NHIN Trial Implementations Document Retrieve Service Interface Specification,
6. NHIN Trial Implementations Audit Log Query Service Interface Specification,
7. NHIN Trial Implementations Consumer Preferences Service Interface Specification
8. NHIN Trial Implementations Health Information Event Messaging Service Interface Specification
9. NHIN Trial Implementations NHIE Service Registry Interface Specification
10. NHIN Trial Implementations Authorized Case Follow-Up Service Interface Specification

It is expected that these core services will be implemented together as a suite since the functional level services are dependent on the foundational services. Specifications #1 through #7 were the focus of the August 2008 testing event and September AHIC demonstrations. Specifications #1 through #9 were included in the November testing and demonstrations during the December 2008 NHIN Trial Implementations Forum.

1.2 Intended Audience

The primary audience for the NHIN Trial Implementations Service Interface Specifications is the individuals responsible for implementing software solutions that realize these interfaces for an NHIE. After reading this specification, one should have an understanding of the context in which the service interface is meant to be used, the behavior of the interface, the Web Services Description Language (WSDLs) used to define the service, any Extensible Markup Language (XML) schemas used to define the content and what “compliance” means from an implementation testing perspective.

1.3 Focus of this Specification

This document presents the NHIN Trial Implementations Audit Log Query Service Interface Specification. The purpose of this specification is to provide the ability to exchange the audit data associated with accessing health information on the NHIN so that consumers and privacy/security officers can account for who has had access to what information for what purpose for use and when they accessed it.

1.3.1 Business Needs Supported by this Specification

This inter-NHIE interface supports the retrieval of audit log data from one NHIE by another NHIE or by a consumer using their PHR to query NHIEs using the NHIN. In particular, it allows security officers and consumers associated with a NHIE to retrieve audit trail data from another NHIE.

This interface specification may also be considered a partial response to the transfer of mitigation (T4) in “IHE IT Infrastructure Technical Framework Supplement 2007-2008 Cross Community Access XCA,” 18.4.2.

1.3.2 Key Attributes of this Specification

1.3.3 Scenarios for Use

1.4 Definitions

1.5 Related Documents

1.6 Relationship to HITSP Constructs

1.7 Relationship to Other NHIN Service Interface Specifications

The Audit Log Query Service Interface is one of the core NHIN service interfaces. See the individual service interface specifications for the specifics of what audit events are generated within the context of those services.

2 Interface Description

2.1 NHIN Interface Descriptive Name:

Audit Log Query Service Interface Specification

2.2 NHIN Interface level:

NHIE to NHIE cross community type of interface

2.3 NHIE Core Services:

2.3.1 Core Services

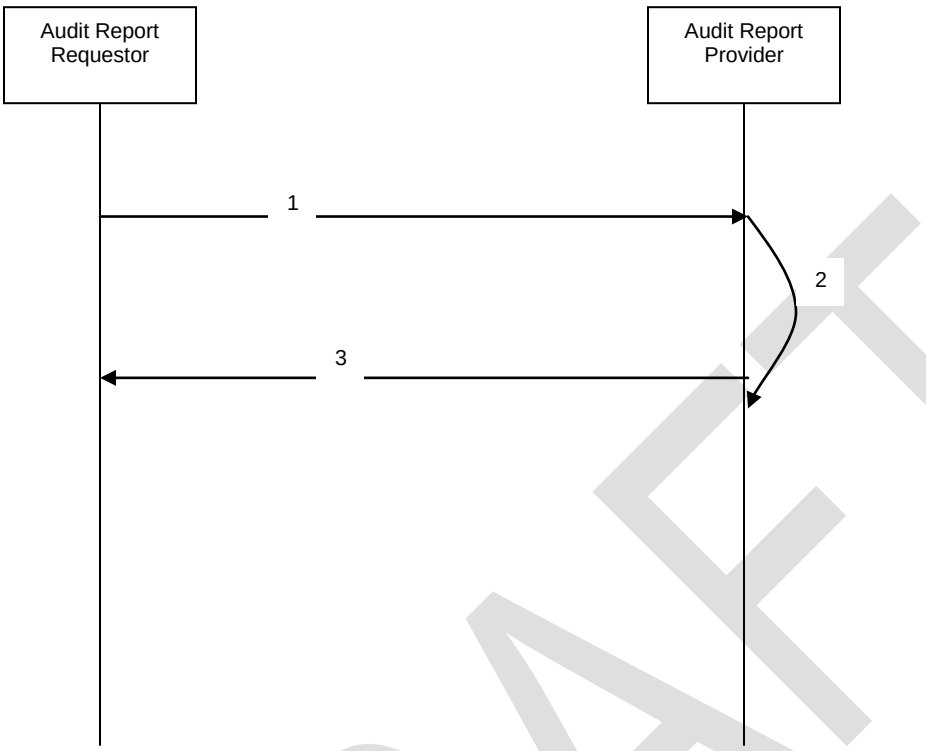
Data Service – Audit Logging

2.3.2 Supported Use Cases

Access to and disclosure of a consumer's PHR information

2.4 Description of Interface

The inter-NHIE interaction that is supported by this interface is described below



1. An *audit report requestor* sends an *audit report request* to the *audit report provider*.

2. The *audit report provider* retrieves the relevant audit trail data from its local audit record repository (ARR). If required, the *audit report provider* transforms the retrieved audit trail data into the required audit report format.

3. The *audit report provider* returns the *audit report* to the *audit report requestor*.

2.5 Technical Pre-conditions

The interface described in this document assumes that the requesting NHIE and the responding NHIE have an established inter-NHIE relationship that conforms to the following specifications:

- NHIN Trial Implementations Messaging Platform Service Interface Specification
- NHIN Trial Implementations Authorization Framework Service Interface Specification
- NHIN Trial Implementations NHIE Service Registry Service Interface Specification
- NHIN Trial Implementations Subject Discovery Service Interface Specification
- NHIN Trial Implementations Query for Documents Service Interface Specification
- NHIN Trial Implementations Retrieve Documents Service Interface Specification
- NHIN Trial Implementations Health Information Event Messaging Service Interface Specification

The interface is applicable to the audit events in these specifications.

It is further assumed that all user and subject identities have been arbitrated prior to the *FindAuditEvents* operation as per

- NHIN Trial Implementations Subject Discovery Service Interface Specification

2.6 Technical Post-conditions

An XML document representing a set of filtered audit log entries is returned by the service provider to the requestor.

3 Interface Definitions

3.1 Message Syntax

See Appendix B for the AuditMessage Schema

3.2 Listing of base standards

- HITSP T15
- IHE Audit Trail Format
  - The IHE Audit Trail Format is based on
    - RFC 3881
    - ASTM E2147-01
    - DICOM Supplement 95
  - See IHE ITI TF 2:3.20.6.2.

3.3 Call Syntax

All inter-NHIE messages in the NHIN are SOAP messages. For the elements associated with an Inter-NHIE interface request/response see the NHIN Trial Implementations Messaging Platform Service Interface Specification.

Appendix C contains a sample of a single AuditMessage that might be returned in the body of a response contained in the typical NHIN SOAP envelope.

3.3.1 WSDL for the *AuditLogQuery* Service

```
<?xml version="1.0" encoding="UTF-8"?>
<wsdl:definitions targetNamespace="http://services.nhin.com"
xmlns:apachesoap="http://xml.apache.org/xml-soap" xmlns:impl="http://services.nhin.com"
xmlns:intf="http://services.nhin.com"
xmlns:audit-message ="http://www.xml.org/xml/schema/7f0d86bd/healthcare-security-audit.xsd"
xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/"
xmlns:wsdlsoap="http://schemas.xmlsoap.org/wsdl/soap/"
xmlns:xsd="http://www.w3.org/2001/XMLSchema">
<!--WSDL created by Apache Axis version: 1.4 Built on Apr 22, 2006 (06:55:48 PDT)-->
 <wsdl:types>
  <schema elementFormDefault="qualified" targetNamespace=http://services.nhin.com
xmlns="http://www.w3.org/2001/XMLSchema">
   <import namespace="http://types.services.nhin.com"/>
   <element name="findAuditEvents">
    <complexType>
     <sequence>
```

```
      <element name="patientId" type="xsd:string"/>
      <element name="userId" type="xsd:string"/>
      <element name="beginDateTime" type="xsd:dateTime"/>
      <element name="endDateTime" type="xsd:dateTime"/>
     </sequence>
    </complexType>
   </element>
   <element name="findAuditEventsResponse">
    <complexType>
     <sequence>
      <element maxOccurs="unbounded" name="findAuditEventsReturn" type="audit-
message:AuditMessage"/>
<!—See Appendix C for schema for AuditMessage from RFC 3881 -->
     </sequence>
    </complexType>
   </element>
  </schema>
  <schema elementFormDefault="qualified" targetNamespace="http://types.services.nhin.com"
xmlns="http://www.w3.org/2001/XMLSchema">
   <complexType name="AuditMessage">
    <sequence/>
   </complexType>
  </schema>
 </wsdl:types>
   <wsdl:message name="findAuditEventsResponse">
      <wsdl:part element="impl:findAuditEventsResponse" name="parameters"/>
   </wsdl:message>
   <wsdl:message name="findAuditEventsRequest">
      <wsdl:part element="impl:findAuditEvents" name="parameters"/>
   </wsdl:message>
   <wsdl:portType name="AuditLogQuery">
      <wsdl:operation name="findAuditEvents">
         <wsdl:input message="impl:findAuditEventsRequest" name="findAuditEventsRequest"/>
         <wsdl:output message="impl:findAuditEventsResponse" name="findAuditEventsResponse"/>
      </wsdl:operation>
   </wsdl:portType>
   <wsdl:binding name="AuditLogQuerySoapBinding" type="impl:AuditLogQuery">
      <wsdlsoap:binding style="document" transport="http://schemas.xmlsoap.org/soap/http"/>
      <wsdl:operation name="findAuditEvents">
         <wsdlsoap:operation soapAction=""/>
         <wsdl:input name="findAuditEventsRequest">
            <wsdlsoap:body use="literal"/>
         </wsdl:input>
         <wsdl:output name="findAuditEventsResponse">
            <wsdlsoap:body use="literal"/>
         </wsdl:output>
      </wsdl:operation>
   </wsdl:binding>
   <wsdl:service name="AuditLogQueryService">
      <wsdl:port binding="impl:AuditLogQuerySoapBinding" name="AuditLogQuery">
         <wsdlsoap:address location="http://localhost:8080/WebServiceProject/services/AuditLogQuery"/>
      </wsdl:port>
   </wsdl:service>
</wsdl:definitions>
```

3.3.2 Constraints/Extensions on the WSDL Parameters

3.3.2.1 FindAuditEvents Parameters

The *FindAuditEvents* operation returns a XML document which conforms to the IHE ATNA Audit Trail format and contains filtered audit log entries.

The *FindAuditEvents* operation's query parameters are purposefully limited so that the audit log query interface does not create an unacceptable disclosure risk itself. The operation supports audit requests by the following paremeters:

Parameter Name	Notes
patientId	The ID of the target Patient
userId	The ID of the target User
beginDateTime	The beginning of the target Date Time range
endDateTime	The end of the target Date Time range

The *FindAuditEvents* operation purposefully does not support requests by other audit event criteria, such as document ID.

It should be noted that for some request, the *patientId* and *userId* will be identical.

The format of the *patientID* shall comply with the NHIN Trial Implementations Query for Document Service Interface Specification.

The implementing NHIE should respond with all audit events that match the parameters.

The service should return an error if the range fails outside of the supported range or the response exceeds maximum audit events.

3.3.2.2 FindAuditEvents Parameters and IHE Audit Trail Format Query Expressions

The *FindAuditEvents* parameters *patientId* and *userId* should be used by service providers to the filter audit repository by applying them as appropriate to the following guiding query expressions.

Note that although the provider may respond with other audit events, they must send *AuditMessage* events that represent disclosures of patient information. Specifically, they must send *AuditMessage* events that match the following expressions:

AuditMessage/EventIdentification/EventTypeCode=EV("ITI-17", "IHE Transactions", "Retrieve Document")

OR

AuditMessage/EventIdentification/EventActionCode='R'

OR

AuditMessage/EventIdentification/EventID=EV (110106, DCM, "Export")

1. *beginDateTime*- and *endDateTime*-Related Filters

Since consideration of the time related parameters is straightforward no particular guidance is described here.

2. *userId* filters

AuditMessage/ActiveParticipant/UserID=$*userId* AND
ActiveParticipation/UserIsRequestor=EV True

Note that this expression applies whether AuditMessage/ActiveParticipant is a User or Human Requestor.

3. *patientId* Filters

AuditMessage/ParticipationObjectIdentification/ ParticipantObjectTypeCode=EV 1 (person)

AND

AuditMessage/ParticipationObjectIdentification/ ParticipantObjectTypeCodeRole=EV 1 (patient)

AND

AuditMessage/ParticipationObjectIdentification/ ParticipantObjectIDTypeCode=EV 2 (patient number)

AND

AuditMessage/ParticipationObjectIdentification/ParticipantObjectID=$*patientId*

3.4 Content Semantics

Content semantics are specified in the above noted base specifications. No additional constraints or extensions over the base specifications at this time.

3.4.1 Content metadata semantics

See the following for applicable audit-related metadata values.

- IHE TF 2:3.16.4.1.5
- IHE TF 2:3.17.4.1.4
- IHE IT Infrastructure Technical Framework Supplement 2007-2008 “Cross-Enterprise Document Sharing-b (XDS.b)”, 3.43.4.1.4
- IHE IT Infrastructure Technical Framework Supplement 2007-2008 “Cross-Enterprise Document Sharing-b (XDS.b)”, 3.43.4.2.4
- “IHE IT Infrastructure Technical Framework Supplement 2007-2008 Cross Community Access XCA,” 3.38.4.1.4.

4 Error Handling

5 Auditing

6 Future Considerations

None identified at this time.

7 Appendix A: WSDL for the AuditLogQuery Service

```
<?xml version="1.0" encoding="UTF-8"?>
<wsdl:definitions targetNamespace="http://services.nhin.com"
xmlns:apachesoap="http://xml.apache.org/xml-soap" xmlns:impl="http://services.nhin.com"
xmlns:intf="http://services.nhin.com"
xmlns:audit-message ="http://www.xml.org/xml/schema/7f0d86bd/healthcare-security-audit.xsd"
xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/"
xmlns:wsdlsoap="http://schemas.xmlsoap.org/wsdl/soap/"
xmlns:xsd="http://www.w3.org/2001/XMLSchema">
<!--WSDL created by Apache Axis version: 1.4 Built on Apr 22, 2006 (06:55:48 PDT)-->
 <wsdl:types>
  <schema elementFormDefault="qualified" targetNamespace=http://services.nhin.com
xmlns="http://www.w3.org/2001/XMLSchema">
   <import namespace="http://types.services.nhin.com"/>
   <element name="findAuditEvents">
    <complexType>
     <sequence>
      <element name="patientId" type="xsd:string"/>
      <element name="userId" type="xsd:string"/>
      <element name="beginDateTime" type="xsd:dateTime"/>
      <element name="endDateTime" type="xsd:dateTime"/>
     </sequence>
    </complexType>
   </element>
   <element name="findAuditEventsResponse">
    <complexType>
     <sequence>
      <element maxOccurs="unbounded" name="findAuditEventsReturn" type="audit-
message:AuditMessage"/>
<!—See Appendix C for schema for AuditMessage from RFC 3881 -->
     </sequence>
    </complexType>
   </element>
  </schema>
  <schema elementFormDefault="qualified" targetNamespace="http://types.services.nhin.com"
xmlns="http://www.w3.org/2001/XMLSchema">
   <complexType name="AuditMessage">
    <sequence/>
   </complexType>
  </schema>
 </wsdl:types>
   <wsdl:message name="findAuditEventsResponse">
      <wsdl:part element="impl:findAuditEventsResponse" name="parameters"/>
   </wsdl:message>
   <wsdl:message name="findAuditEventsRequest">
      <wsdl:part element="impl:findAuditEvents" name="parameters"/>
   </wsdl:message>
   <wsdl:portType name="AuditLogQuery">
      <wsdl:operation name="findAuditEvents">
         <wsdl:input message="impl:findAuditEventsRequest" name="findAuditEventsRequest"/>
         <wsdl:output message="impl:findAuditEventsResponse" name="findAuditEventsResponse"/>
      </wsdl:operation>
   </wsdl:portType>
   <wsdl:binding name="AuditLogQuerySoapBinding" type="impl:AuditLogQuery">
```

```
    <wsdlsoap:binding style="document" transport="http://schemas.xmlsoap.org/soap/http"/>
    <wsdl:operation name="findAuditEvents">
      <wsdlsoap:operation soapAction=""/>
      <wsdl:input name="findAuditEventsRequest">
        <wsdlsoap:body use="literal"/>
      </wsdl:input>
      <wsdl:output name="findAuditEventsResponse">
        <wsdlsoap:body use="literal"/>
      </wsdl:output>
    </wsdl:operation>
  </wsdl:binding>
  <wsdl:service name="AuditLogQueryService">
    <wsdl:port binding="impl:AuditLogQuerySoapBinding" name="AuditLogQuery">
      <wsdlsoap:address location="http://localhost:8080/WebServiceProject/services/AuditLogQuery"/>
    </wsdl:port>
  </wsdl:service>
</wsdl:definitions>
```

8 Appendix B - AuditMessage Schema[1]

```
<!-- edited with XMLSPY v2004 rel. 3 U (http://www.xmlspy.com) by Glen F. Marshall (HL7 Technical
Steering Committee) -->
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema" elementFormDefault="qualified"
attributeFormDefault="unqualified">
	<xs:element name="AuditMessage">
		<xs:complexType>
			<xs:sequence>
				<xs:element name="EventIdentification" type="EventIdentificationType"/>
				<xs:element name="ActiveParticipant" maxOccurs="unbounded">
					<xs:complexType>
						<xs:complexContent>
							<xs:extension base="ActiveParticipantType"/>
						</xs:complexContent>
					</xs:complexType>
				</xs:element>
				<xs:element name="AuditSourceIdentification"
type="AuditSourceIdentificationType" maxOccurs="unbounded"/>
				<xs:element name="ParticipantObjectIdentification"
type="ParticipantObjectIdentificationType" minOccurs="0" maxOccurs="unbounded"/>
			</xs:sequence>
		</xs:complexType>
	</xs:element>
	<xs:complexType name="EventIdentificationType">
		<xs:sequence>
			<xs:element name="EventID" type="CodedValueType"/>
			<xs:element name="EventTypeCode" type="CodedValueType" minOccurs="0"
maxOccurs="unbounded"/>
		</xs:sequence>
		<xs:attribute name="EventActionCode" use="optional">
			<xs:simpleType>
				<xs:restriction base="xs:string">
					<xs:enumeration value="C">
						<xs:annotation>
							<xs:appinfo>Create</xs:appinfo>
						</xs:annotation>
					</xs:enumeration>
					<xs:enumeration value="R">
						<xs:annotation>
							<xs:appinfo>Read</xs:appinfo>
						</xs:annotation>
					</xs:enumeration>
					<xs:enumeration value="U">
						<xs:annotation>
							<xs:appinfo>Update</xs:appinfo>
						</xs:annotation>
					</xs:enumeration>
					<xs:enumeration value="D">
						<xs:annotation>
							<xs:appinfo>Delete</xs:appinfo>
						</xs:annotation>
					</xs:enumeration>
```

[1] Reproduced from http://www.xml.org/xml/schema/7f0d86bd/healthcare-security-audit.xsd. See also RFC 3881 §6.1.

```
                                        <xs:enumeration value="E">
                                                <xs:annotation>

        <xs:documentation>Execute</xs:documentation>
                                                </xs:annotation>
                                        </xs:enumeration>
                                </xs:restriction>
                        </xs:simpleType>
                </xs:attribute>
                <xs:attribute name="EventDateTime" type="xs:dateTime" use="required"/>
                <xs:attribute name="EventOutcomeIndicator" use="required">
                        <xs:simpleType>
                                <xs:restriction base="xs:integer">
                                        <xs:enumeration value="0">
                                                <xs:annotation>
                                                        <xs:appinfo>Success</xs:appinfo>
                                                </xs:annotation>
                                        </xs:enumeration>
                                        <xs:enumeration value="4">
                                                <xs:annotation>
                                                        <xs:appinfo>Minor failure</xs:appinfo>
                                                </xs:annotation>
                                        </xs:enumeration>
                                        <xs:enumeration value="8">
                                                <xs:annotation>
                                                        <xs:appinfo>Serious failure</xs:appinfo>
                                                </xs:annotation>
                                        </xs:enumeration>
                                        <xs:enumeration value="12">
                                                <xs:annotation>
                                                        <xs:appinfo>Major failure; action made
unavailable
        </xs:appinfo>
                                                </xs:annotation>
                                        </xs:enumeration>
                                </xs:restriction>
                        </xs:simpleType>
                </xs:attribute>
        </xs:complexType>
        <xs:complexType name="AuditSourceIdentificationType">
                <xs:sequence>
                        <xs:element name="AuditSourceTypeCode" type="CodedValueType"
minOccurs="0" maxOccurs="unbounded"/>
                </xs:sequence>
                <xs:attribute name="AuditEnterpriseSiteID" type="xs:string" use="optional"/>
                <xs:attribute name="AuditSourceID" type="xs:string" use="required"/>
        </xs:complexType>
        <xs:complexType name="ActiveParticipantType">
                <xs:sequence minOccurs="0">
                        <xs:element name="RoleIDCode" type="CodedValueType" minOccurs="0"
maxOccurs="unbounded"/>
                </xs:sequence>
                <xs:attribute name="UserID" type="xs:string" use="required"/>
                <xs:attribute name="AlternativeUserID" type="xs:string" use="optional"/>
                <xs:attribute name="UserName" type="xs:string" use="optional"/>
```

```
<xs:attribute name="UserIsRequestor" type="xs:boolean" use="optional" default="true"/>
<xs:attribute name="NetworkAccessPointID" type="xs:string" use="optional"/>
<xs:attribute name="NetworkAccessPointTypeCode" use="optional">
	<xs:simpleType>
		<xs:restriction base="xs:unsignedByte">
			<xs:enumeration value="1">
				<xs:annotation>
					<xs:appinfo>Machine Name, including DNS
name</xs:appinfo>
				</xs:annotation>
			</xs:enumeration>
			<xs:enumeration value="2">
				<xs:annotation>
					<xs:appinfo>IP Address</xs:appinfo>
				</xs:annotation>
			</xs:enumeration>
			<xs:enumeration value="3">
				<xs:annotation>
					<xs:appinfo>Telephone Number</xs:appinfo>
				</xs:annotation>
			</xs:enumeration>
		</xs:restriction>
	</xs:simpleType>
</xs:attribute>
</xs:complexType>
<xs:complexType name="ParticipantObjectIdentificationType">
	<xs:sequence>
		<xs:element name="ParticipantObjectIDTypeCode" type="CodedValueType"/>
		<xs:choice minOccurs="0">
			<xs:element name="ParticipantObjectName" type="xs:string"
minOccurs="0"/>
			<xs:element name="ParticipantObjectQuery" type="xs:base64Binary"
minOccurs="0"/>
		</xs:choice>
		<xs:element name="ParticipantObjectDetail" type="TypeValuePairType"
minOccurs="0" maxOccurs="unbounded"/>
	</xs:sequence>
	<xs:attribute name="ParticipantObjectID" type="xs:string" use="required"/>
	<xs:attribute name="ParticipantObjectTypeCode" use="optional">
		<xs:simpleType>
			<xs:restriction base="xs:unsignedByte">
				<xs:enumeration value="1">
					<xs:annotation>
						<xs:appinfo>Person</xs:appinfo>
					</xs:annotation>
				</xs:enumeration>
				<xs:enumeration value="2">
					<xs:annotation>
						<xs:appinfo>System object</xs:appinfo>
					</xs:annotation>
				</xs:enumeration>
				<xs:enumeration value="3">
					<xs:annotation>
						<xs:appinfo>Organization</xs:appinfo>
					</xs:annotation>
```

```
                        </xs:enumeration>
                        <xs:enumeration value="4">
                                <xs:annotation>
                                        <xs:appinfo>Other</xs:appinfo>
                                </xs:annotation>
                        </xs:enumeration>
                </xs:restriction>
        </xs:simpleType>
</xs:attribute>
<xs:attribute name="ParticipantObjectTypeCodeRole" use="optional">
        <xs:simpleType>
                <xs:restriction base="xs:unsignedByte">
                        <xs:enumeration value="1">
                                <xs:annotation>
                                        <xs:appinfo>Patient</xs:appinfo>
                                </xs:annotation>
                        </xs:enumeration>
                        <xs:enumeration value="2">
                                <xs:annotation>
                                        <xs:appinfo>Location</xs:appinfo>
                                </xs:annotation>
                        </xs:enumeration>
                        <xs:enumeration value="3">
                                <xs:annotation>
                                        <xs:appinfo> Report</xs:appinfo>
                                </xs:annotation>
                        </xs:enumeration>
                        <xs:enumeration value="4">
                                <xs:annotation>
                                        <xs:appinfo>Resource</xs:appinfo>
                                </xs:annotation>
                        </xs:enumeration>
                        <xs:enumeration value="5">
                                <xs:annotation>
                                        <xs:appinfo>Master file</xs:appinfo>
                                </xs:annotation>
                        </xs:enumeration>
                        <xs:enumeration value="6">
                                <xs:annotation>
                                        <xs:appinfo>User</xs:appinfo>
                                </xs:annotation>
                        </xs:enumeration>
                        <xs:enumeration value="7">
                                <xs:annotation>
                                        <xs:appinfo>List</xs:appinfo>
                                </xs:annotation>
                        </xs:enumeration>
                        <xs:enumeration value="8">
                                <xs:annotation>
                                        <xs:appinfo>Doctor</xs:appinfo>
                                </xs:annotation>
                        </xs:enumeration>
                        <xs:enumeration value="9">
                                <xs:annotation>
                                        <xs:appinfo>Subscriber</xs:appinfo>
```

```
                </xs:annotation>
            </xs:enumeration>
            <xs:enumeration value="10">
                <xs:annotation>
                    <xs:appinfo>Guarantor</xs:appinfo>
                </xs:annotation>
            </xs:enumeration>
            <xs:enumeration value="11">
                <xs:annotation>
                    <xs:appinfo>Security User Entity</xs:appinfo>
                </xs:annotation>
            </xs:enumeration>
            <xs:enumeration value="12">
                <xs:annotation>
                    <xs:appinfo>Security User Group</xs:appinfo>
                </xs:annotation>
            </xs:enumeration>
            <xs:enumeration value="13">
                <xs:annotation>
                    <xs:appinfo>Security Resource</xs:appinfo>
                </xs:annotation>
            </xs:enumeration>
            <xs:enumeration value="14">
                <xs:annotation>
                    <xs:appinfo>Security Granualarity
Definition</xs:appinfo>
                </xs:annotation>
            </xs:enumeration>
            <xs:enumeration value="15">
                <xs:annotation>
                    <xs:appinfo>Provider</xs:appinfo>
                </xs:annotation>
            </xs:enumeration>
            <xs:enumeration value="16">
                <xs:annotation>
                    <xs:appinfo>Report Destination</xs:appinfo>
                </xs:annotation>
            </xs:enumeration>
            <xs:enumeration value="17">
                <xs:annotation>
                    <xs:appinfo>Report Library</xs:appinfo>
                </xs:annotation>
            </xs:enumeration>
            <xs:enumeration value="18">
                <xs:annotation>
                    <xs:appinfo>Schedule</xs:appinfo>
                </xs:annotation>
            </xs:enumeration>
            <xs:enumeration value="19">
                <xs:annotation>
                    <xs:appinfo>Customer</xs:appinfo>
                </xs:annotation>
            </xs:enumeration>
            <xs:enumeration value="20">
                <xs:annotation>
```

```
                                        <xs:appinfo>Job</xs:appinfo>
                                    </xs:annotation>
                                </xs:enumeration>
                                <xs:enumeration value="21">
                                    <xs:annotation>
                                        <xs:appinfo>Job Stream</xs:appinfo>
                                    </xs:annotation>
                                </xs:enumeration>
                                <xs:enumeration value="22">
                                    <xs:annotation>
                                        <xs:appinfo>Table</xs:appinfo>
                                    </xs:annotation>
                                </xs:enumeration>
                                <xs:enumeration value="23">
                                    <xs:annotation>
                                        <xs:appinfo>Routing Criteria</xs:appinfo>
                                    </xs:annotation>
                                </xs:enumeration>
                                <xs:enumeration value="24">
                                    <xs:annotation>
                                        <xs:appinfo>Query</xs:appinfo>
                                    </xs:annotation>
                                </xs:enumeration>
                            </xs:restriction>
                        </xs:simpleType>
                    </xs:attribute>
                    <xs:attribute name="ParticipantObjectDataLifeCycle" use="optional">
                        <xs:simpleType>
                            <xs:restriction base="xs:unsignedByte">
                                <xs:enumeration value="1">
                                    <xs:annotation>
                                        <xs:appinfo>Origination / Creation</xs:appinfo>
                                    </xs:annotation>
                                </xs:enumeration>
                                <xs:enumeration value="2">
                                    <xs:annotation>
                                        <xs:appinfo>Import / Copy from original
</xs:appinfo>
                                    </xs:annotation>
                                </xs:enumeration>
                                <xs:enumeration value="3">
                                    <xs:annotation>
                                        <xs:appinfo>Amendment</xs:appinfo>
                                    </xs:annotation>
                                </xs:enumeration>
                                <xs:enumeration value="4">
                                    <xs:annotation>
                                        <xs:appinfo>Verification</xs:appinfo>
                                    </xs:annotation>
                                </xs:enumeration>
                                <xs:enumeration value="5">
                                    <xs:annotation>
                                        <xs:appinfo>Translation</xs:appinfo>
                                    </xs:annotation>
                                </xs:enumeration>
```

```
                                <xs:enumeration value="6">
                                        <xs:annotation>
                                                <xs:appinfo>Access / Use</xs:appinfo>
                                        </xs:annotation>
                                </xs:enumeration>
                                <xs:enumeration value="7">
                                        <xs:annotation>
                                                <xs:appinfo>De-identification</xs:appinfo>
                                        </xs:annotation>
                                </xs:enumeration>
                                <xs:enumeration value="8">
                                        <xs:annotation>
                                                <xs:appinfo>Aggregation, summarization,
derivation</xs:appinfo>
                                        </xs:annotation>
                                </xs:enumeration>
                                <xs:enumeration value="9">
                                        <xs:annotation>
                                                <xs:appinfo>Report</xs:appinfo>
                                        </xs:annotation>
                                </xs:enumeration>
                                <xs:enumeration value="10">
                                        <xs:annotation>
                                                <xs:appinfo>Export / Copy to
target</xs:appinfo>
                                        </xs:annotation>
                                </xs:enumeration>
                                <xs:enumeration value="11">
                                        <xs:annotation>
                                                <xs:appinfo>Disclosure</xs:appinfo>
                                        </xs:annotation>
                                </xs:enumeration>
                                <xs:enumeration value="12">
                                        <xs:annotation>
                                                <xs:appinfo>Receipt of disclosure</xs:appinfo>
                                        </xs:annotation>
                                </xs:enumeration>
                                <xs:enumeration value="13">
                                        <xs:annotation>
                                                <xs:appinfo>Archiving</xs:appinfo>
                                        </xs:annotation>
                                </xs:enumeration>
                                <xs:enumeration value="14">
                                        <xs:annotation>
                                                <xs:appinfo>Logical deletion</xs:appinfo>
                                        </xs:annotation>
                                </xs:enumeration>
                                <xs:enumeration value="15">
                                        <xs:annotation>
                                                <xs:appinfo>Permanent erasure / Physical
destruction </xs:appinfo>
                                        </xs:annotation>
                                </xs:enumeration>
                        </xs:restriction>
                </xs:simpleType>
```

```
                </xs:attribute>
                <xs:attribute name="ParticipantObjectSensitivity" type="xs:string" use="optional"/>
        </xs:complexType>
        <xs:complexType name="CodedValueType">
                <xs:attribute name="code" type="xs:string" use="required"/>
                <xs:attributeGroup ref="CodeSystem"/>
                <xs:attribute name="displayName" type="xs:string" use="optional"/>
                <xs:attribute name="originalText" type="xs:string" use="optional"/>
        </xs:complexType>
        <xs:complexType name="TypeValuePairType">
                <xs:attribute name="type" type="xs:string" use="required"/>
                <xs:attribute name="value" type="xs:base64Binary" use="required"/>
        </xs:complexType>
        <xs:attributeGroup name="CodeSystem">
                <xs:attribute name="codeSystem" type="OID" use="optional"/>
                <xs:attribute name="codeSystemName" type="xs:string" use="optional"/>
        </xs:attributeGroup>
        <xs:simpleType name="OID">
                <xs:restriction base="xs:string">
                        <xs:whiteSpace value="collapse"/>
                </xs:restriction>
        </xs:simpleType>
</xs:schema>
```

9 Appendix C - Sample AuditMessage

Sample Request

See the NHIN Trial Implementations Messaging Platform Service Interface Specification for the elements associated with an Inter-NHIE interface request.

Sample Response

See the NHIN Trial Implementations Messaging Platform Service Interface Specification for the elements associated with an Inter-NHIE interface response.

The following is a single AuditMessage that might be returned in the body of a response:


```
<AuditMessage xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="healthcare-security-audit.xsd">
        <EventIdentification EventActionCode="E" EventDateTime="2008-01-10T13:46:51.140-05:00"
EventOutcomeIndicator="0">
                <EventID code="110112" codeSystemName="DCM" displayName="Query"/>
    <EventTypeCode code="ITI-18" codeSystemName="IHE Transactions" displayName="Registry
Stored Query"/>
        </EventIdentification>
   <ActiveParticipant NetworkAccessPointTypeCodeError=""
      UserID="XdsTester" UserIsRequestor="true" NetworkAccessPointID="192.168.254.16">
                        <RoleIDCode code="110153" codeSystemName="DCM"
displayName="Source"/>
   </ActiveParticipant>
   <ActiveParticipant NetworkAccessPointTypeCodeError=""
UserID="http://129.6.24.109:9080/axis2/services/xdsregistryb" UserIsRequestor="false">
      <RoleIDCode code="110152" codeSystemName="DCM" displayName="Destination"/>
   </ActiveParticipant>
   <AuditSourceIdentification AuditSourceID="92.97.127.202"/>
   <ParticipantObjectIdentification ParticipantObjectID=" 543797436^^^&1.2.840.113619.6.197&ISO"
ParticipantObjectTypeCode="2" ParticipantObjectTypeCodeRole="24">
      <ParticipantObjectIDTypeCode code="ITI-18" codeSystemName="IHE Transactions"
         displayName="Registry Stored Query"/>
<ParticipantObjectQuery>PHF1ZXJ5OkFkaG9jUXVlcnlSZXF1ZXN0CiAgICB4bWxuczpxdWVyeT0idXJuO
m9hc2lzOm5hbWVzOnRjOmVieG1sLXJlZ3JlcDp4c2Q6cXVlcnk6My4wIiB4bWxuczpyaW09InVybjpvYXN
pczpuYW1l
czp0YzplYnhtbC1yZWdyZXA6eHNkOnJpbTozLjAiPgogICAgPHF1ZXJ5OlJlc3BvbnNlT3B0aW9uIHJldHV
ybkNvbXBvc2VkT2JqZWN0cz0idHJ1ZSIgcmV0dXJuVHlwZT0iTGVhZkNsYXNzIi8+CiAgICA8cmltOkFka
G9jUXVlcnkgaWQ9InVybjp1dWlkOjE0ZDRkZWJmLThmOTctNDI1MS05YTc0LWE5MDAxNmIwYWYwZ
CI+CiAgICAgICAgPHJpbTpTbG90IG5hbWU9IiRYRFNEb2N1bWVudEVudHJ5U3RhdHVzIj4KICAgICAgI
CAgICAgPHJpbTpWYWx1ZUxpc3Q+CiAgICAgICAgICAgICAgICA8cmltOlZhbHVlPigndXJuOm9hc2lzOm
5hbWVzOnRjOmVieG1sLXJlZ3JlcDpTdGF0dXNUeXBlOkFwcHJvdmVkJyk8L3JpbTpWYWx1ZT4KICAgI
CAgICAgPC9yaW06VmFsdWVMaXN0PgogICAgICAgIDwvcmltOlNsb3Q+CiAgICAgICAgPHJpbTpT
bG90IG5hbWU9IiRYRFNEb2N1bWVudEVudHJ5UGF0aWVudElkIj4KICAgICAgICAgICAgPHJpbTpWYW
x1ZUxpc3Q+CiAgICAgICAgICAgICAgICA8cmltOlZhbHVlPicyNzBhNTlkN2E4YjE0NWJeXl4mYW1wOzEu
My42LjEuNC4xLjIxMzY3LjIwMDUuMy43JmFtcDtJU08nPC9yaW06VmFsdWU+CiAgICAgICAgICAgIDwvvc
mltOlZhbHVlTGlzdD4KICAgICAgICA8L3JpbTpTbG90PgogICAgPC9yaW06QWRob2NRdWVyeT4KPC9x
dWVyeTpBZGhvY1F1ZXJ5UmVxdWVzdD4K
      </ParticipantObjectQuery>
   </ParticipantObjectIdentification>
</AuditMessage>
```

10 Appendix D – Example Scenarios

10.1 Story Background

The Audit Query Service provides a means for Privacy and Security Officers to be able to request and review audit trail data from NHIEs. It also creates a means whereby a consumer may request and review audit trail data from using their PHR as the platform to mount such a request to the NHIN for audit trail data.

10.1.1 Scene 1

In this scene the Privacy/Security Officer requests audit trail data from another NHIE. There are two possible means of doing this; the request can be made in one step or two steps.

10.1.1.1 Example 1a: Security Officer Requests Remote Audit Trail (Two Steps)

1. Security officer Z (in NHIE A) wants to reconstruct the audit trail for clinician Y.
2. Security officer Z uses an audit report browser to request an audit trail report from NHIE A.
3. NHIE A responds with a local audit trail report. The local audit trail report shows that, during the target time interval, clinician Y used an EHR in NHIE A to retrieve a medical summary for patient X in NHIE B (a NHIE with which NHIE A has an established inter-NHIE relationship).
4. Therefore, security officer Z uses the audit report browser to request from NHIE A that it request an audit trail report from the NHIE B with the following filters: The *user* is clinician Y, *patient* is patient X and *date time range* is the target time interval.
5. **NHIE A requests the audit trail report from NHIE B.**
6. **NHIE B responds to NHIE A with an audit trail report that shows all relevant audit events that match the criteria.**
7. NHIE A forwards the audit trail report to security officer Z.
8. Security officer Z views the audit trail report in her browser.

Alternatively, the security officer can view local and remote data in one step.

10.1.1.2 Example 1b: Security Officer Requests Remote Audit Trail (One Step)

1. Security officer Z (in NHIE A) wants to reconstruct the audit trail for clinician Y.
2. Security officer Z uses an audit report browser to request an audit trail report from NHIE A.
3. While retrieving the local audit trail report, NHIE A determines that the local audit report shows that clinician Y requested and received a medical summary for patient X from NHIE B.
4. NHIE A (automatically) requests a remote audit trail report from NHIE B (filtered by clinician Y and the target time interval.).
5. NHIE B returns the remote audit trail report to NHIE A.

6. NHIE A aggregates the remote audit trail report with the local audit trail report.

7. NHIE A returns the aggregated audit trail report to the audit report browser.

8. Security officer Z views the aggregated audit trail report.

10.1.2 Scene 2

In this scenario a consumer using their PHR requests and views audit trail data from the NHIN.

10.1.2.1 Example 2: Consumer Uses PHR to View Cross-NHIE Disclosure Information

1. Person N uses her PHR (in NHIE B) to request a disclosure report, i.e. an audit trail report that shows all access events associated with her health record during a target time interval.

2. NHIE B processes the request by retrieving access event data from its local audit record repository (ARR). While analyzing the local disclosure data, NHIE B determines that one of the access events in the target time interval was a response from NHIE A to a request (from NHIE B) for Person N's medical summary.

3. **NHIE B requests a remote audit rail report from NHIE A (filtered by Person N and the target time interval).**

4. **NHIE A processes the request and responds to NHIE B with the audit trail report.**

5. NHIE B aggregates the local and remote reports and sends the aggregated report to the PHR.