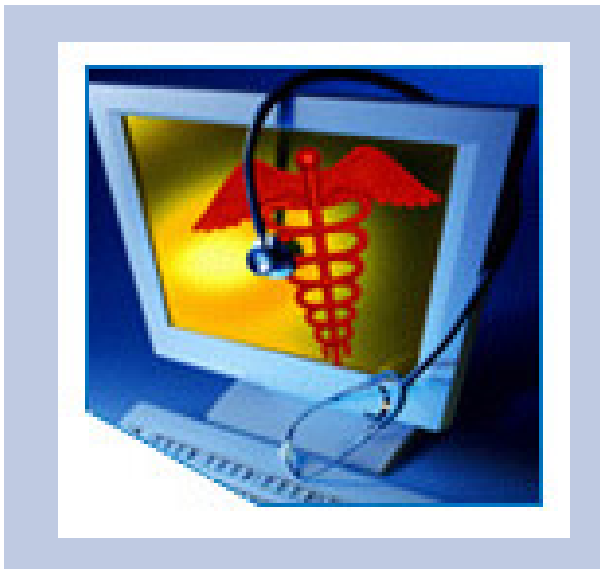# HITSP Interoperability Specification:
Notification of Document Availability (NAV) Transaction

HITSP/IST-29

Submitted to:

Healthcare Information Technology Standards Panel

Submitted by:

Electronic Health Records Technical Committee
Biosurveillance Technical Committee

DOCUMENT CHANGE HISTORY

Version Number	Description of Change	Name of Author	Date Published
1.0	Final Draft	Electronic Health Record Technical Committee Biosurveillance Technical Committee	August 18, 2006

1.0 FOREWORD

Healthcare Information Technology Standards Panel (HITSP) is a multi-stakeholder coordinating body designed to provide the process within which affected parties can identify, select, and harmonize standards for communicating healthcare information throughout the healthcare spectrum. HITSP functions as a partnership of the public and private sectors and operate with a neutral and inclusive governance model administered by the American National Standards Institute. The goal of the panel is to:

- Facilitate the development of harmonized interoperability specifications and information policies, including SDO work products (e.g. standards, technical reports). These policies, profiles and work products are essential for establishing privacy, security and interoperability among healthcare software applications.
- Coordinate, as appropriate, with other national, regional and international groups addressing healthcare informatics to ensure that the resulting standards are globally relevant.
- Be use-case driven, utilize information from stakeholders and base its decisions on industry needs.

The HITSP shall serve the public good by working to ensure that the combined work of various healthcare information standards organizations supports interoperability, accurate use, access, privacy and security of shared health information.

In order to advance the goal of expanding harmonized interoperability specifications and information policies, HITSP was tasked with developing interoperability specifications for three main use case "breakthroughs areas" in which specific, near term value to the health care consumer could be realized. The harmonized use case areas are:

1.	Biosurveillance	Transmit essential ambulatory care and emergency department visit, utilization, and lab result data from electronically enabled health care delivery and public health systems in standardized and anonymized format to authorized Public Health Agencies with less than one day lag time.
2.	Consumer Empowerment	Allow consumers to establish and manage permissions access rights and informed consent for authorized and secure exchange, viewing, and querying of their linked patient registration summaries and medication histories between designated caregivers and other health professionals.
3.	Electronic Health Record	Allow ordering clinicians to electronically access laboratory results, and allow non-ordering authorized clinicians to electronically access historical and other laboratory results for clinical care.

The interoperability specification provides a detailed mapping of existing standards and specifications such as implementation guides, integration profiles to actions and actors that satisfy the requirements imposed by the relevant use cases. It identifies and constrains standards where necessary, and creates groupings of specific actions and actors to further describe the relevant contexts. Where gaps and

overlaps are identified, the interoperability specification provides recommendations and a roadmap for corrections to be made.

2.0 INTRODUCTION

65 **2.1 OVERVIEW**

This Notification of Document Availability (**NAV**) transaction specification references the structures and the work that is accomplished by implementing this transaction. Source material was predominantly from the "Integrating the Healthcare Enterprise (IHE) Cross-Document Sharing (XDS) IT Infrastructure (ITI) Technical Framework (TF) NAV" supplement. This transaction specifications references:

70 The Notification of Document Availability Profile (NAV) introduces a mechanism allowing notifications to be sent point-to-point to systems within a Cross-Enterprise Document Sharing affinity domain (See "IHE IT Infrastructure XDS Integration Profile"), eliminating the need for manual steps or polling mechanisms for a Document Consumer to be aware that documents that may be of interest have been registered with an XDS Document Registry Actor.

75 The capability for automation of critical workflows used in healthcare has been greatly advanced by the introduction of the Cross-Enterprise Document Sharing Integration Profile. However, without point-to-point notification of document availability, these workflows still require manual interactions between parties using document sharing.

This basic mechanism is only intended to facilitate the common part of a large range of workflows related
80 to notifying a remote party (user or system) that one or more documents have been registered in an XDS Registry and may be retrieved if the notified party wishes.

Related Documents	Document Description	Document Name and Location
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (TF)	Volume 1 (ITI TF-1) Integration Profiles Revision 2 August 15, 2005	www.IHE.net
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (TF)	Volume 2 (ITI TF-2) Transactions Revision 2 August 15, 2005	www.IHE.net
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (TF) Supplement	Supplement (ITI TF-Supplement) ITI-25 Notification of Document Availability (NAV), IHE TF Jun 28, 2005	www.IHE.net

2.2 AUDIENCE

The interoperability specification is designed to be used by analysts who need to understand the interoperability requirements for the described use case, and by implementers working to develop interoperable applications. Understanding and using the relevant interoperability set of specifications is a key requirement for establishing interoperability compliance.

2.3 TERMS AND DEFINITIONS

The definitions used for the purposes of this document can be found in the glossary. Refer to glossary in the appendix.

2.4 CONVENTIONS

This specification uses the following to convey the full descriptions and usage of standards:

UML sequence and activity diagrams

In these diagrams, the actors and transactions are highlighted within the framework of the specific scenario or context. The actors involved in the specified use-scenario or context are mapped out, and the interactions between each action and actor for a particular context, and the flow of data are provided through the use of arrows. Diagrams are named according to the section in which they reside, and will use the following naming convention:

Figure <section number>-<consecutive number for the diagram, e.g. 1, 2, 3, etc.>. <Short name/description of diagram>. For example, a diagram residing in section 3.1.3 showing the Actor Interactions for the Send Lab Results transaction package is named:
Figure 3.1.3-1. Send Lab Results Transaction Package

Tables

Tables are used to indicate standards categorizations, as well as dependencies and constraints between constructs. Tables are named according to the section in which they reside, and will use the following naming convention:

Table <section number>-<consecutive number for the table, e.g. 1, 2, 3, etc.>. <Short name/description of table>. For example, a table residing in section 2.7.1 showing the Dependencies between the transactions for the Send Lab Results transaction package is named:
Table 2.7.1-1. Send Lab Results Transaction Package dependencies

References

When references are made to another section within an Interoperability Specification a section number is used by itself. When references are made to other constructs that are related to the Interoperability Specification, such as Transaction Packages, Components or Composite Standards, the HITSP document short name and section number are displayed as follows:

<HITSP Document short name or Composite Standard Short Name>-<Volume Number>: <section number>

where:

<HITSP document short name> is a short designator for the construct (e.g. HITSP/ISTP-013)

<Composite Standard Short Name> is a short designator for the composite standard (e.g. IHE-ITI TF)

<Volume Number> is the applicable volume within the given composite standard (e.g. 1)

<section number> is the applicable section number (e.g. 3.1)

For example: HITSP/ISTP-013: 3.1 refers to Section 3.1 in the Interoperability Specification for a Transaction Package, IHE-ITI TF-2: 4.33 refers to Section 4.33 in volume 2 of the IHE IT Infrastructure Technical Framework.

Reproductions

Where large sections of composite standards or base standards are reproduced within a HITSP specification, the reproduced sections are cited with introductory text containing the reference information for the composite or base standard. In addition, the beginning and ending of the reproduced text are respectively shown using a beginning statement:

The text for the <composite or base standard name> specification begins here:

And an ending statement:

The text for the <composite or base standard name> ends here.

2.5 COMMENTS

To submit comments for this interoperability specification, please download the Comment Submission sheet from the HITSP site at www.hitsp.org and provide all relevant information, and then email the completed document to hitspcomments@ansi.org. Comments are consolidated periodically and sent to the Technical Committees for review.

2.6 COPYRIGHT PERMISSIONS

COPYRIGHT NOTICE

IHE materials used in this document have been extracted from relevant copyrighted materials with
160 permission of Integrating the Healthcare Enterprise (IHE). Copies of this standard may be retrieved from the IHE website at www.ihe.net.

2.7 LIST OF COMPOSITE STANDARDS

Composite Standard	Description
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (TF)	"IHE IT Infrastructure 2005-2006 Supplement for Trial Implementation" ITI-25 Notification of Document Availability Integration Profile (NAV), IHE TF Jun 28, 2005

165 ### 2.8 LIST OF COMPONENTS AND TRANSACTIONS

The following list of components and transactions and their definitions are used by the transaction specification.

Transaction Name	Description	Document Reference	Date Added
HITSP/IST-029	Notiifcation of Lab Result Availability	IST-HITSP-29-v1.0-2007	8/18/06

170

2.8.1 <u>DEPENDENCIES</u>

Integration Profile	Depends on	Dependency Type	Purpose
Notification of Document Availability	Cross Enterprise Document Sharing	An XDS Actor must be grouped with the initiating NAV Notification Sender and the final NAV Notification Receiver.	Required to initiate the first transaction, and to perform any useful work as a result.

175 **NOTE: The above table is from the IHE TF NAV supplement**

2.9 CONSTRAINTS

Not applicable

180
3.0 TRANSACTIONS

3.1 CONTEXT OVERVIEW

3.1.1 CONTEXTUAL CONSTRAINTS

185   The NAV operations assume that a suitable security and privacy environment has been established. Almost all of the relevant threats will be managed by agreements, policies, and technologies that are external to the NAV transactions. The threats and security objectives that must be addressed are described in Appendix K of Volume II of IHE-IT-TF. That is where the requirements for the sharing of documents are described. There are only a few issues that are unique and apply to the NAV profile.

190   The NAV messages have been designed to minimize the patient identifying or private information content. They convey only:

    • The UUIDs of documents that have been made available,

    • The location of the registry where these documents are described,

    • Free text instructions for the recipient,

195   • The email address of the sender, and

    • The email address of the recipient.

This reveals very little information. It does reveal that a relationship exists between sender and recipient, and the volume of traffic may indicate more about the nature of this relationship. The NAV profile does not expect this information to be protected, so when the mere existence of a relationship between sender and

200   recipient must be concealed the use NAV profile is not appropriate. For many of the expected use cases the relationships involved are public information, e.g., it is not a secret that a laboratory system will have messages for a referring physician.

The actual exchange of documents and their associated security considerations is discussed in the XDS profile. The NAV use of email for notifications is different from the XDS use of email for registry

205   submissions performed in off-line mode.

The risks that are specific to the NAV profile are:

    1. Unauthorized recipient for the notification. This could be from a variety of causes, and must be managed primarily by administrative procedures. This risk is mitigated by the design of the NAV messages. They have a minimum of protected information so that the unauthorized disclosure

210   does not reveal protected information.

    2. Incorrect recipient. This is similar to the unauthorized recipient, except that the recipient is authorized to receive the messages. For example, when there are several possible recipients for notification an erroneous selection will send the notification to the wrong recipient. This risk must be mitigated by proper applications design, training, and administrative procedures.

215   3. Traffic monitoring. Email traffic is easily monitored, and the notifications will traverse unprotected networks. The messages have been designed to minimize the patient information, but the pattern of messages will reveal the relationships of the senders and receivers. The message contents do indicate the number of documents being exchanged, which may also reveal

the nature of the relationships. This risk is mitigated by avoiding the use of NAV for relationships
220   that must be kept private.

4. Malicious message modification. This is can be a denial of service threat, or part of a deception
effort. Notifications could be modified to cause notifications to be lost. This risk is mitigated by
using the signature portion of the message. Using either information provided in the optional
"keyinfo" attribute or information that is exchanged independently, the signature can confirm that
225   the manifest information has not been modified and that the documents have not been modified.
This does not prevent destruction of messages, but it will indicate when messages have been
modified.

5. Corrupted messages, e.g. from a denial of service effort. This risk is also mitigated by use of
the signature information. It does not prevent corruption, but does indicate that messages have
230   been corrupted so that external administrative steps can be taken to protect the email systems.

3.1.2   TECHNICAL ACTORS

Actor	Description
Notification Sender	This actor sends notifications of availability for documents in an XDS registry, and receives acknowledgements of these notifications.
Notification Receiver	This actor receives notifications of availability for documents in an XDS registry, and may optionally send acknowledgments of them.
SMTP Aether	This actor is shown for completeness, but is really part of the SMTP Infrastructure of the Internet.

235   ### 3.1.3   ACTOR INTERACTIONS

Figure 12.2-1 shows the actors directly involved in the NAV Integration Profile and the relevant
transactions between them. Other actors that may be indirectly involved due to their participation in other
profiles are not necessarily shown.

Figure 12.2-1. Actor Diagram

240
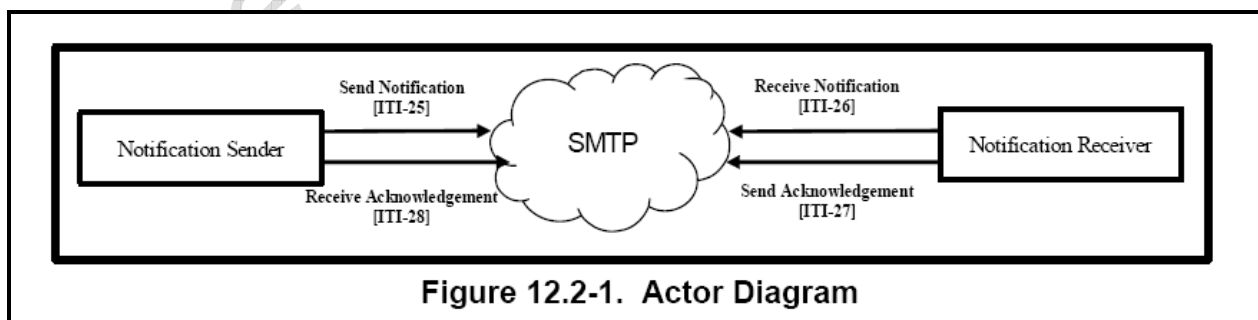
NOTE: The above figure is from the IHE TF NAV supplement

Table 12.2-1 lists the transaction for each actor directly involved in the NAV Profile. In order to claim
support of this Integration Profile, an implementation must perform the required transactions (labeled "R").

Transactions labeled "O" are optional. A complete list of options defined by this Integration Profile and that implementations may choose to support is listed in Volume I, Section 12.3.

Table 12.2-1. Actors and Transactions

Actors	Transactions	Optionality	Section in Vol. 2
Notification Sender	Send Notification	R	3.25
	Receive Acknowledgement	O	3.28
Notification Receiver	Receive Notification	R	3.26
	Send Acknowledgement	O	3.27

NOTE: The above table is from the IHE TF NAV supplement

Options that may be selected for this Integration Profile are listed in the table 12.3-1 along with the Actors to which they apply. Dependencies between options when applicable are specified in notes.

Actor	Options	Vol & Section
Notification Sender	Acknowledgement Request with SMTP Option[2]	Vol II, Section 3.28
	Acknowledgement Request with POP3 Option[4]	Vol II, Section 3.28
	Acknowledgement Request with IMAP Option[4]	Vol II, Section 3.28
Notification Receiver	Send Acknowledgement Option	Vol II, Section 3.28
	Receive Notification with SMTP Option[3]	Vol II, Section 3.26
	Receive Notification with POP3 Option[5]	Vol II, Section 3.26
	Receive Notification with IMAP Option[5]	Vol II, Section 3.26

NOTE: The above table is from the IHE TF NAV supplement
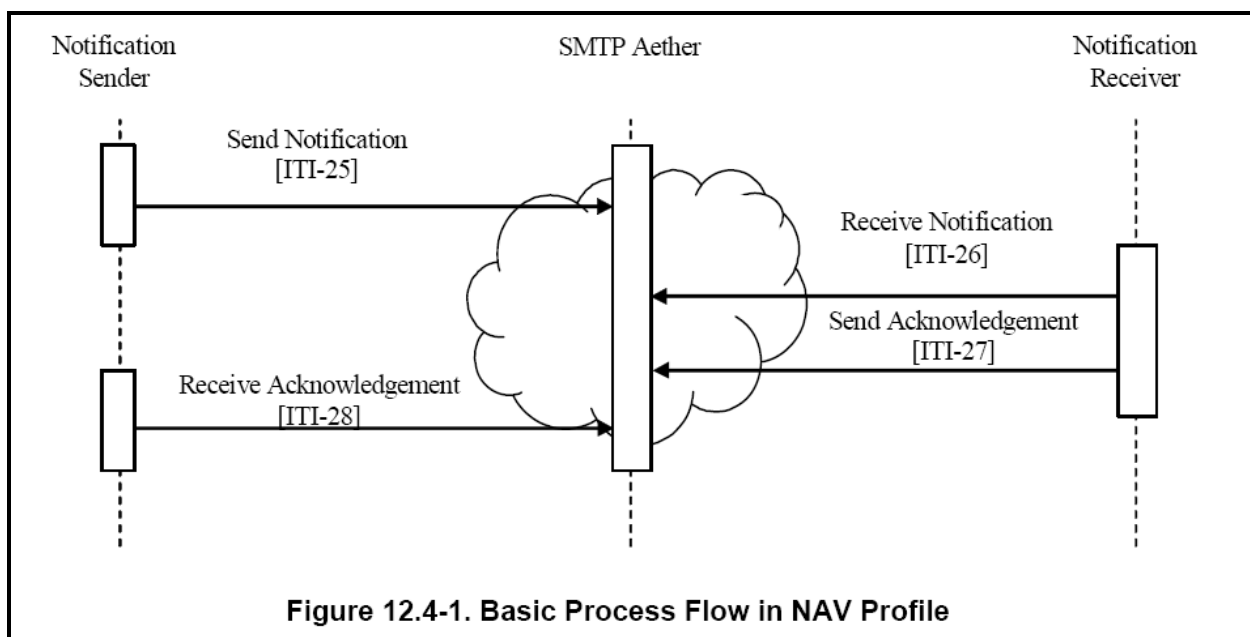
3.2 PROCESS FLOWS

Figure 12.4-1. Basic Process Flow in NAV Profile

NOTE: The above figure is from the IHE TF NAV supplement

260

Send Notification: This transaction provides for sending of document availability notices in an XDS Affinity Domain.

Receive Notification: This transaction provides for receipt of document availability notices in an XDS Affinity Domain.

265 **Send Acknowledgement:** This transaction provides for sending of acknowledgements to document availability notices in an XDS Affinity Domain.

Receive Acknowledgement: This transaction provides for receipt of acknowledgements of document availability notices in an XDS Affinity Domain.

Clinical exemplars are available in the IHE TF specification.

270

3.2.1 PROCESS PRE-CONDITIONS

When grouped with the secure node actor, the Notification Sender and Notification Receiver Actors within this profile may, but are not required to use secure communications for notifications between two healthcare providers because no protected health information (PHI) is contained within the content exchanged. Similarly, because no PHI is transferred, the actors are not required to log the export of PHI; however they are not prohibited from logging the transaction.

In the case where the notifications involve the patient, there are some security issues to be addressed. An e-mail message directed to or sent by a patient most likely contains the identity of the patient. The information becomes even more sensitive when the sender or receiver of the notification is a person or

280   organization that specializes in certain types of healthcare, such as4 substance abuse treatment or
        psychiatric care.

        XDS Affinity Domains and their members must consider these issues carefully when supporting patient
        notification or intermediation of notifications using this profile. See section 12.6 of IHE-ITI-TF-NAV   on
        Security Impacts for more details.

285   The starting point of a notification must have some relationship with an XDS Actor. Otherwise, there is no
        source for the information to be sent. The ending point would typically also be related to an XDS
        Document Consumer Actor or subsequent utility of the notification received will be minimal5. Intermediate
        actors do not require any association with an XDS Actor or XDS Affinity Domain.

        Before the notification message can be fully constructed, the Notification Sender actor must identify the
290   recipient of the message. The PWP and PDQ profiles may be of some assistance in identifying the e-mail
        address of providers or patients. However, there are no specific requirements that a Notification Sender
        Actor be grouped with any PWP or PDQ actors even when they are available.

        Note: This profile does not address how the recipients of the message are to be selected. This is an
        administrative function outside of the scope of this profile. What makes a receiver unique is that they have
295   a unique e-mail address. Whether this is a person or a node is not material to this profile.

3.2.1.1   PROCESS TRIGGERS

An XDS Registry a Notification Sender uses this transaction to send notifications about documents of
interest:

300   • Upon the registration of new documents.

                • Upon the need to notify about existing documents.

Notification Receivers are free to specify the event that triggers the initiation of a Receive

305   3.2.2   PROCESS POST-CONDITIONS

Notification transaction. The following are example triggers:

                • An end user may request that the Notification Receiver check for new notifications.

                • The Notification Receiver may periodically poll for new notifications.

                • The Notification Receiver may be notified of incoming mail by an external mechanism.

310

A receiver implementing the Send Acknowledgement option must send this message upon receipt of any
XDS Notification message that requests acknowledgement to indicate that the message has been
received.

An end-user may initiate the sending of an acknowledgement upon viewing the message and activating
315   the embedded mailto link.

A receiver must not send this message unless the sender has requested acknowledgements in the original notification message.

3.2.2.1   PROCESS OUTPUTS

320   None.

3.3   DATA FLOWS

Not applicable.

325   # 4.0 CONSTRAINTS FOR REUSE

Not Applicable

5.0 APPENDIX

5.1   GLOSSARY

330   This is the HITSP glossary that spans all the interoperability specifications, which can be found in the following folder on the HITSP site:
http://publicaa.ansi.org/sites/apdl/Documents/Forms/AllItems.aspx?RootFolder=http%3a%2f%2fpublicaa%2eansi%2eorg%2fsites%2fapdl%2fDocuments%2fStandards%20Activities%2fHealthcare%20Informatics%20Technology%20Standards%20Panel

335