Integrating the Healthcare Enterprise

IHE IT Infrastructure
Technical Framework Supplement

Mobile Alert Communication Management (mACM)

Draft for Public Comment

Date: June 8, 2015
Author: IHE ITI Technical Committee
Email: iti@ihe.net

Please verify you have the most recent version of this document. See here for Trial Implementation and Final Text versions and here for Public Comment versions.

Foreword

This is a supplement to the IHE IT Infrastructure Technical Framework V11.0. Each supplement undergoes a process of public comment and trial implementation before being incorporated into the volumes of the Technical Frameworks.

This supplement is published on June 8, 2015 for public comment. Comments are invited and can be submitted at http://www.ihe.net/ITI_Public_Comments. In order to be considered in development of the trial implementation version of the supplement, comments must be received by July 8, 2015.

This supplement describes changes to the existing technical framework documents.

"Boxed" instructions like the sample below indicate to the Volume Editor how to integrate the relevant section(s) into the relevant Technical Framework volume.

Amend Section X.X by the following:

Where the amendment adds text, make the added text **bold underline**. Where the amendment removes text, make the removed text **~~bold strikethrough~~**. When entire new sections are added, introduce with editor's instructions to "add new text" or similar, which for readability are not bolded or underlined.

General information about IHE can be found at: http://ihe.net.

Information about the IHE IT Infrastructure domain can be found at: http://ihe.net/IHE_Domains.

Information about the organization of IHE Technical Frameworks and Supplements and the process used to create them can be found at: http://ihe.net/IHE_Process and http://ihe.net/Profiles.

The current version of the IHE IT Infrastructure Technical Framework can be found at: http://ihe.net/Resources/Technical_Frameworks.

CONTENTS

Introduction to this Supplement

This introduces the Mobile Alert Communication Management Profile. The mACM Profile provides the infrastructural components needed to send short, unstructured text alerts to human recipients and records the outcomes of any human interactions upon receipt of the alert. The mACM Profile additionally allows for a feedback mechanism to determine the status of an alert through the use of alert statuses. Additional characteristics of alerts are discussed in X.1.4.1.

Recognizing that there are many health care workflows that could leverage a notification mechanism, it is not the aim of this profile to describe all of these workflows. Instead, this profile will limit considerations to two Content Modules in support the following workflows:

- *Crisis Response*, defined in X.4.2.1, covers the distribution of notifications to health workers defined by the Common Alerting Protocol version 1.2.
- *Care Reminders*, defined in X.4.2.2, covers the distribution of notifications to care givers and subjects of care based on upcoming or missed appointments as defined, medication reminders and other similar patient care reminders.

It is the expectation that the infrastructural components of the mACM Profile will be reusable beyond the use cases described here within and will support extensions to support domain specific workflows.

Open Issues and Questions

#0) Should a codeset be defined to capture the priority of an alert in the flag.priority resource.

#1) Would we be prescriptive about the way to set PCD abnormality flags in the flag.characterstics data field? Table 8.3 is referenced, but no uri or oid is specified.

#2) mACM defines FHIR® extensions which require profiles in 3.X01.41.2.1and 3.X02.41.2.1. FHIR® requires that these profiles are published. Currently the text states that the profiles are available at, for example:

http://www.ihe.net/fake_url_for_public_comment/mACM/Profile/flag.recipient

these URLs are examples only. Upon publication, a permanent home for any needed extension points should be defined as an IHE resource.

#3) Do not have a way to identity a device which is a non-medical device (e.g., not subject to FDA regulation) A clarification issue on FHIR® was raised:

http://gforge.hl7.org/gf/project/fhir/tracker/?action=TrackerItemEdit&tracker_item_id=6209&start=0

#4) Should we have Device as a recipient in transactions X01 and X02. This is not specifically required for the uses cases described in Vol 1, but may be useful for PCD.

#5) For the flag.author data field, it would be useful to have the author of an alert be an Organization resource (e.g., CDC). A FHIR® issue was filed:

http://gforge.hl7.org/gf/project/fhir/tracker/?action=TrackerItemEdit&tracker_item_id=6208&start=0

If this Issue is not approved, an extension point should be added to the flag resource to allow an Organizational author of the alert. For example the following could be added to Table 3.X01.4.2.2.1-1:

`extension [0..1]`	This data field identifies the originator of the alert. This data field is defined as an extension with URL `flag.author` and with value in `valueReference` and whose value is an organization represented by a reference to an `Organization` resource. This data field should only be populated if a subject of care was not identified.	`Reference( Organization )`

#6) MEMLS has location notion of physical offset (e.g., within building). How should this be represented for the dissemination event location field? See Appendix A of PCD MEM-LS Supplement.

#7) The use of the flag.category is unclear – it could either be flag/alert content or could be used for alert filtering/routing. A FHIR® issue was filed:

http://gforge.hl7.org/gf/project/fhir/tracker/?action=TrackerItemEdit&tracker_item_id=6170&start=0

to clarify its use. A FHIR® Skype conversation indicated that the later sense of flag.category is what is intended, and this is the way that is used in this profile.

#8) Use Case #1 in Vol 1 requires that an alert be issued without an identified subject of care. The flag resource has a flag.patient field that is [1..1] which would preclude the use of the flag resource for this use case. A FHIR® issue has been filed:

http://gforge.hl7.org/gf/project/fhir/tracker/?action=TrackerItemEdit&tracker_item_id=6171&start=0

to change to [0..1]. If this CP is approved, then Section 3.X01.4.1.2.1 should be updated.

#9) A concern brought up by PCD is that the use of flag.patient is limiting scope of the alert. What about location or equipment source=medical device, a use cased highlighted in Vol 1 of PCD? Example of a location would be a cord pull in bathroom in a hallway. A FHIR® issue was raised:

http://gforge.hl7.org/gf/project/fhir/tracker/?action=TrackerItemEdit&tracker_item_id=6271&start=0

#10) Multiple extension points have been define by this profile on the FHIR® flag resource. Some of those may be useful to be part of the core resource. A FHIR® issue to this effect was raised here:

http://gforge.hl7.org/gf/project/fhir/tracker/?action=TrackerItemEdit&tracker_item_id=6272&start=0

#11) Open Issue: mACM definition of "alert" is not same as general definition: http://ihe.net/uploadedFiles/Documents/Templates/IHE_TF_GenIntro_AppD_Glossary_Rev1.0_2014-07-01.pdf

It is not clear how to resolve: For example, PCD's term could be broadened or we could rewrite this profile to not use the term alert.

Closed Issues

Feb 25, 2015: Should we reference ACM is much as possible (e.g., in Actor and Transaction descriptions), or pull in text as a service to the reader? Decision: Pull in the text for the ease of the reader. This will also help if there is a potential conflict between ACM and mACM Actor requirements. Any such conflicts should be reviewed and resolved as part of public comment.

Mar 23, 2015: Various standards were considered for the transaction specification in Vol 2. These standards were assessed according to the matrix: http://wiki.ihe.net/index.php?title=MACM_Volume2_Standards_Assessment
Consensus was reached to use FHIR® DSTU v2 for the two transactions to be specified.

Feb 24, 2015: The "Emergent Results" use case will be considered out of scope for the time being. This could be revisited during the public comment period.

Feb 24, 2015: For dissemination of alerts, it is expected that PCD-06 and PCD-07 transactions will be sufficient. On this assumption, no assessment will be performed on the standards available for the transactions between the Alert Manager and Alert Communicator Actors at this time.

Feb 18, 2015: The Query For Alert status is somewhat similar to the PCD-05 transaction in that it is a way to report alert statuses from AM to AR. PCD-05 was cut from final text. However PCD-05 does not meet our requirements for doing analytics on the AR side.

Feb 18, 2015: It was discussed whether or not the existing PCD-04 Report Alert transaction could be used instead of the new ITI-X01 "mACM Report Alert" transaction. PCD-04 is an HL7®v2 message for clinical observations. It was decided that using this would be semantically incorrect as we have many uses cases that are not observations.

Nov 20, 2014:

- Consensus: we will narrow to two use cases/healthcare workflows involving notifications (preferably on the next call).
- Recommendation: to have a clinical workflow (about a specific subject of care) and public health/health system management workflow (not about a subject of care).

- Consensus: Critical findings workflow use case is to radiological specific. Derrick E. will draft new one.
- Consensus: ~~Triggered Notifications – Integrated Care Plans: The HIE issues reminders to subjects of care and/or care providers regarding pending guideline-informed activities and regarding non-adherence to care plans – both errors of commission and errors of omission.~~ Cut for lack of clarity(from Introductory text)
- Consensus: For each of the use-cases/workflows, the behavior of each actor should be described in high level terms in the relevant "X.4.2.1.2 <simple name> Process Flow" section.
- Question: (Mick T.) Will this include notifications about intrusion detection into the HIE? *Not specifically. If there was no existing system for communicating such notifications in the HIE, the infrastructural components are expected to be reusable to communicate the notification. A "notification publisher" actor would be the system monitoring the HIE (e.g., through queryable-ATNA) and producing the notification for a list of recipients. This type of workflow could be specified in a future work-cycle.*

December 4, 2014 Call Notes

- Question (Carl L) What is the retention policy for notification and notification receipts?
- Answer (Gila P): retention policies usually left up to jurisdiction.
- Question (Elliott S) Would list of health workers (and/or subjects of care) include contact information:
  Answer (Rob H/Carl L): Yes, can have multiple
  Post-Call Response (Carl L): This needs more discussion as to who should know contact information for recipients. Simplest thing is perhaps the Notification Consumer/Receiver.
- Question (Rob H): who is responsible for prioritization of which contact point to use?
  Answer (Carl L): Envisioned that this is the responsibility of the Notification Consumer/Receiver
- Question (Rob H): What about an existing AP that knows the prioritization of the contact point?
- Answer (Carl L): Example -- The AP would first submit the notification to a primary contact point (e.g., email). If there is no ACK of the notification after a set period of time, the message content can be sent again to a secondary contact point (e.g., cell phone)
- Question (Rob H): In the CAP/Crisis Response use case, what is the nature of the ACK.
  Answer (Carl L): It is an acknowledgement by the human that they have read the notification. Should require an active confirmation ('click to confirm'), not just a passive "I saw it on the screen."
- Question (Rob H): How notifications in this context different than those in PCD

Answer (Carl L): There is a feedback option which allows recording of human interactions.

- Question (Carl L): In two use cases (Critical Findings and Crisis Response) there is an ACK by the human that the alert is received. Are these to be treated differently? Answer (Rob H): Though syntactically they can be the same, they semantically differ. In the Critical Findings use case, the meaning of the ACK in radiology is that the radiologist reviewed the findings with the patient and there is informed consent. In the Crisis Response use case, it is that the human has read and understood the notification.
- Remark (Lynn F): Should reconsider names of actors to avoid collision with existing actors in other profiles. There is Notification Consumer - in the PCD Notification Communication Mgmt Profile. Notification Message Receiver & Notification Message Transmitter Actors were used in a HITSP Emergency Msg Distribute Element document. Response (Carl L): Updated actor names for group feedback.

General Introduction

Update the following Appendices to the General Introduction as indicated below. Note that these are not appendices to Volume 1.

Appendix A - Actor Summary Definitions

Add the following actors to the IHE Technical Frameworks General Introduction list of Actors:

Actor	Definition
Alert Reporter (AR)	This actor originates the alert (an alarm, either physiological or technical, or an advisory).
Alert Manager (AM)	This actor receives alerts from the Alert Reporter (AR), manages them, and dispatches them to the AC Actor
Alert Communicator (AC)	This actor receives alerts from the Alert Manager (AM) Actor. Endpoint devices are connected either directly or indirectly to the Alert Communicator (AC) Actor. The Alert Communicator (AC) may utilize a locally controlled or public infrastructure. See IHE PCD TF-I 6.3.4.

Appendix B - Transaction Summary Definitions

Add the following transactions to the IHE Technical Frameworks General Introduction list of Transactions:

Transaction	Code	Definition
Mobile Report Alert	ITI-X01	This transaction is used by the Alert Reporter to report alerts to the Alert Manager (AM). The Alert Reporter (AR) sends alerts to the Alert Manager (AM) Actor in an unsolicited manner.
Disseminate Alert	PCD-06	This transaction is used by Alert Manager (AM) to disseminate the alert to the Alert Communicator (AC). This transaction is specified in PCD TF-2: 3.6.
Report Dissemination Alert Status	PCD-07	This transaction is used by Alert Communicator to report one or more dissemination status updates and/or replies to the Alert Manager (AM). A single Report Alert for Devices transaction from the AM to the AC can result in numerous Report Dissemination Alert Status for Mobile Devices transactions from the AC back to the AM. This transaction is specified in PCD TF-2: 3.7.
Query for Alert Status	ITI-X02	This transaction is used by the Alert Reporter (AR) to query an Alert Manager (AM) for alert status information as communicated from an Alert Consumer (AC) to an Alert Manager (AM) for a particular alert.

Glossary

Add the following glossary terms to the IHE Technical Frameworks General Introduction Glossary:

No new glossary terms.

Volume 1 – Profiles

Copyright Licenses

Add the following to the IHE Technical Frameworks General Introduction Copyright section:

None.

Domain-specific additions

None.

X Mobile Alert Communication Management (mACM) Profile

This introduces the Mobile Alert Communication Management (mACM) Profile. The mACM Profile provides an extension to the Patient Care Devices (PCD) - Alert Communication Management (ACM) Profile. These extensions:

- provide alternative message semantics for the Report Alert transaction, which is suitable for mobile devices and non-clinical contexts;
- define a new transaction, Query for Alert Status, which allows an originator of an alert to receive all status updates on alert that it reported;
- support alerting in national deployment and cross-enterprise contexts in addition to a controlled health delivery network;
- support interaction with the public, such as appointment reminders, on a broad a variety of devices, interaction timings and platforms.

X.1 Mobile Alert Communication Management (mACM) Actors, Transactions, and Content Modules

This section defines the actors, transactions, and/or content modules in this profile. General definitions of actors are given in the Technical Frameworks General Introduction Appendix A at http://www.ihe.net/Technical_Framework/index.cfm.

Figures X.1-1 shows the actors directly involved in the ACM and mACM Profiles and the relevant transactions between them.

No content modules are defined by the mACM Profile.

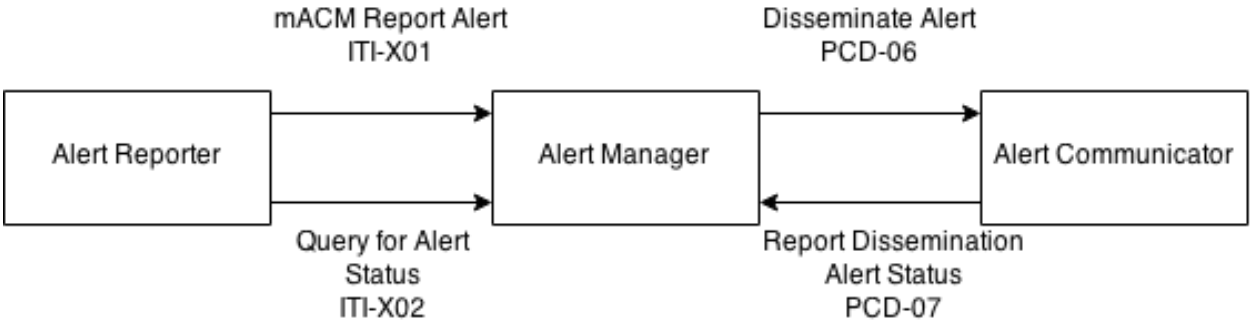


Figure X.1-1: mACM Actor and Transaction Diagram

Table X.1-1 lists the transactions for each actor directly involved in the mACM 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 X.1-1: mACM Profile - Actors and Transactions

Actors	Transactions	Optionality	Reference
Alert Reporter	Mobile Report Alert	R	3.X01
	Query for Alert Status	O	3.X02
Alert Manager	Mobile Report Alert	R	3.X01
	Disseminate Alert	R	IHE PCD TF 2:3.4
	Report Dissemination Alert Status	R	IHD PCD TF 2:3.7
	Query for Alert Status	R	3.X02
Alert Communicator	Disseminate Alert	R	IHE PCD TF 2:3.4
	Report Dissemination Alert Status	R	IHE PCD TF 2:3.7

X.1.1 Actor Descriptions and Actor Profile Requirements

Most requirements are documented in Transactions (Volume 2). This section documents any additional requirements on profile's actors.

The semantics and data types used to represent alert type, alert priority, alert inactivation state and escalation and de-escalation of priority in the messages of this actor are based on IEC 60601-1-8 definitions (see IHE PCD TF-2:3.4).

X.1.1.1 Alert Reporter

This actor originates the alert (an alarm, either physiological or technical, or an advisory).

This profile specifies communication of the data produced by this actor. This actor may optionally cancel an outstanding alert condition, or an outstanding alert condition may be optionally escalated via a follow-on alert.

This actor may aggregate and adapt alerts from multiple sources as needed to make them interoperable with the Alert Manager Actor. It does not need to be the original source of the alert data.

In large alert source populations, an aggregation system may be useful for concentration and possible alert coordination (smart alerting).

X.1.1.2 Alert Manager

This actor receives alerts from the Alert Reporter, manages them, and dispatches them to the Alert Consumer Actor.

The message semantics for the Disseminate Alert transaction used in the communication of the data to/from the Alert Manager Actor and the Alert Communicator Actor is the Wireless Communication Transfer Protocol (WCTP) as defined in IHE PCD TF-2.

X.2 mACM Actor Options

Options that may be selected for each actor in this profile, if any, are listed in the Table X.2-1. Dependencies between options when applicable are specified in notes.

Table X.2-1: mACM - Actors and Options

Actor	Option Name	Reference
Alert Reporter	Query for Alert Status	X.2.1
Alert Manager	No options defined	--
Actor Consumer	No options defined	--

X.2.1 Query for Alert Status Option

The Query for Alert Status Option is the mechanism whereby a creator of an alert can receive feedback on the current status of the alert. This option is available to support analytics on the delivery status of alerts as well as to provide feedback capabilities for other business processes that an Alert Reporter may wish to implement. An Alert Reporter Actor may participate in this option by initiating the Query for Alert Status transaction.

X.3 mACM Required Actor Groupings

No Actor Groupings are defined in the mACM Profile.

X.4 mACM Overview

The mACM Profile supports the delivery of a variety of alert to both Health Workers and Clients (Subjects of Care) with a feedback mechanism to record delivery status and human responses.

X.4.1 Concepts

In Figure X.4.1-1 the sequencing of the transactions in Figure X.1-1 is illustrated.

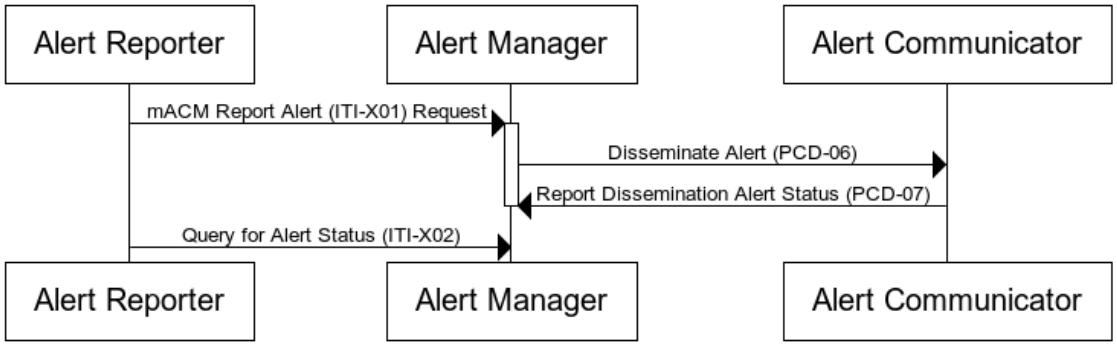


Figure X.4-1: Process Flow Diagram

X.4.2 Use Cases

The mACM Profile takes into consideration uses cases that span clinical, health systems management and public health domains.

A critical requirement of the mACM Profile is the ability to provide basic alerting services within resource-constrained environments with a low barrier to entry. Such communities may exist at national context for Low and Middle Income Countries (LMICs[1]), as well as underserved communities in high-income countries (e.g., the population targeted by Detroit's Beacon Project[2]). A proliferation of alerting services exists in national health networks of resource-constrained countries (see Figure X.4.2-1 for an illustrative example) and the mACM Profile fulfills an important need by the ministries of health to provide a central messaging infrastructure. Such a centralized infrastructure provides the ministry the ability to:

- Assert and enforce governance policies on the utilization of alerting services on mobile platforms
- Define and enforce cost control measures across various mobile alerting platforms

[1] http://data.worldbank.org/about/country-and-lending-groups

[2] http://www.healthit.gov/sites/default/files/beacon-factsheet-semi.pdf

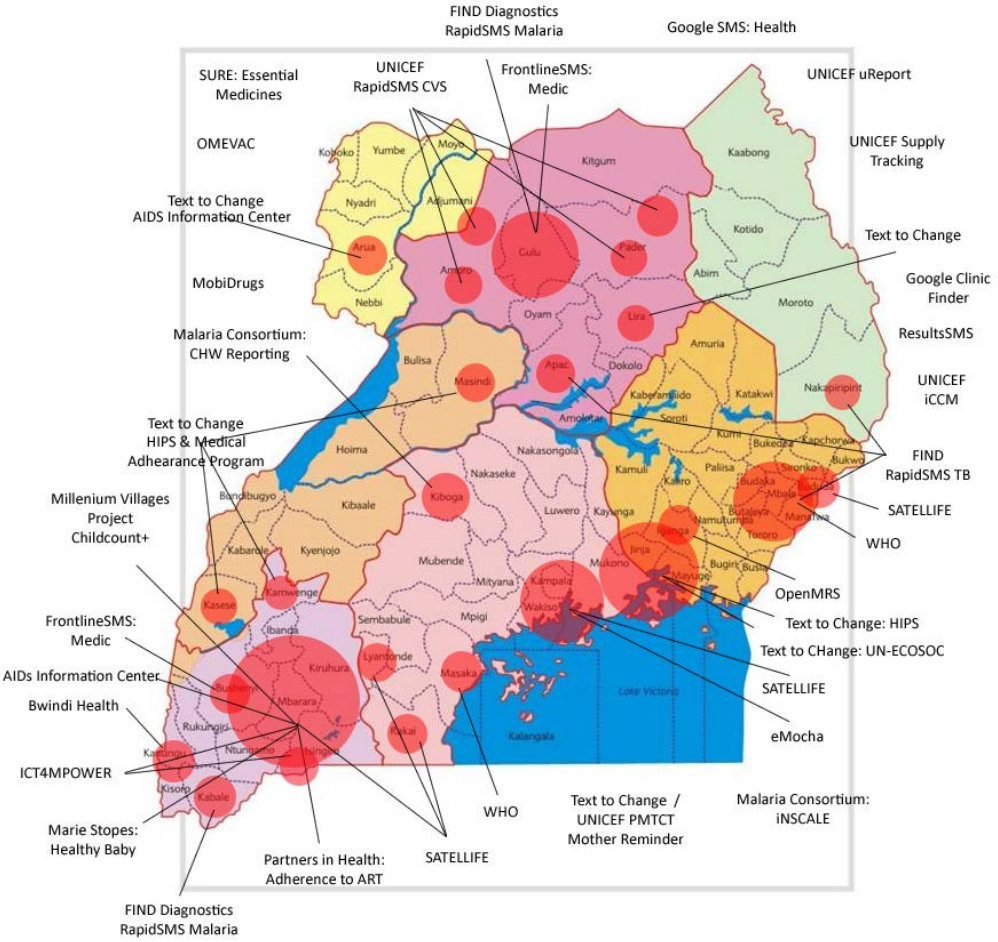


Figure X.4.2-1 Extant mobile based Alerting Services in Uganda

(Courtesy UNICEF/Blaschke/2011)

X.4.2.1 Use Case #1: Crisis Response

In response to a crisis or emergency situation, such as the recent outbreaks of Ebola in western Africa, it is critical to communicate to health workers across organizational and national boundaries, and to verify receipt of such alerts. Such alerts are commonly issued in the OASIS Common Alerting Protocol (CAP) format:

- http://docs.oasis-open.org/emergency/cap/v1.2/CAP-v1.2-os.html

There is a desire to assure human acknowledgment of receipt of these CAP messages.

X.4.2.1.1 Crisis Response Use Case Description

The Crisis Response use case describes the mechanism for delivering alerts in the CAP format to health workers within a particular health care network. The nature of this network is not prescribed in this profile and may consist, for example of a network of hospitals or a national health care network.

The manner of production and publication of the CAP message is not prescribed in this profile.

There are several existing profiles and specifications related to CAP messages that details values of and requirements on particular data fields. Such specifications include:

- OASIS Integrated Public Alert and Warning System (IPAWS)
- HiTSP T 63 - Emergency Message Distribution Element Transaction
- NIEM Emergency Management

This profile can be used to deliver CAP messages issued by an appropriate authority to an appropriate set of health workers on last-mile devices. In addition, this profile describes a mechanism for recording human acknowledgment of receipt of information contained in the CAP messages. These response can it turn be used for analytical and monitoring purposes.[3]

X.4.2.1.2 Crisis Response Process Flow

The workflow for delivery and acknowledgment of a CAP message is illustrated in Figure X.4.2.1.2-1.

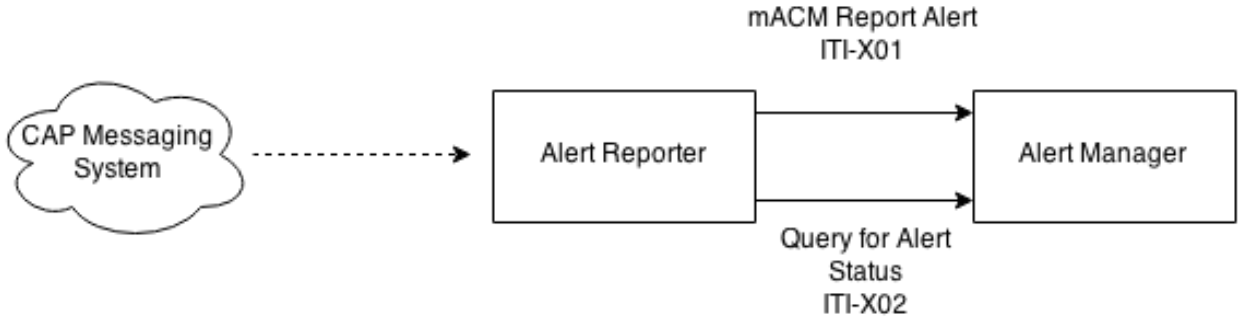


Figure X.4.2.1.2-1: CAP Delivery and Acknowledge

Figure X.4.2.1.2-1 illustrate the distribution of CAP message from an external system to an Alert Reporter. Though the method for receiving a CAP message is not specified by the profile, the Alert Reporter should:

[3] Waidyanatha, Nuwan and Gow, Gordon and Anderson, Peter, Common Alerting Protocol Message Broker for Last-Mile Hazard Warning System in Sri Lanka: An Essential Component (May 2007). Available at SSRN: http://ssrn.com/abstract=1568001 or http://dx.doi.org/10.2139/ssrn.1568001

- Identify a cohort of health workers for the receiving the text of the CAP message
- Render the CAP message in a suitable manner for reporting to an Alert Manager

The Alert Manager distributes the alert and collects alert dissemination statuses from Alert Communicators and makes status information available to the Alert Reporter via the Query for Alert Status.

X.4.2.2 Use Case #2: Care Reminders

A subject of care may receive care from multiple providers across multiple health care networks, and coordination of care across providers and networks is difficult. If a Longitudinal Health Record (or Shared Health Record) is present, Care Reminder alerts can be triggered through the examination of clinical records about the subject of care. Care Reminder alerts are sent either to the subject of care or a designated health worker.

X.4.2.2.1 Care Reminder Use Case Description

The following are illustrative examples of Care Reminder alerts:

- (Rwanda): When a patient is referred to the district hospital by a Community Health Worker they can choose to be referred as immediate, urgent or routine. In urgent cases they must visit the hospital within three days and for routine referrals they must visit the hospital within seven days. The Health Information Exchange (HIE) is able to detect if the patient has missed their referral by checking if an encounter has been received at the Longitudinal Health Record within the time frame. If an encounter has not been received the HIE sends out an out an alert of the missed appointment to inform the Community Health Worker that originally interfaced with that patient.
- (Tanzania) An examination of an Electronic Medical or Health Record indicates that a child has missed a vaccination according to an established protocol of care. An SMS reminder is generated and sent to the mother or other designated guardian. In the case when a mother does not have access to a cell-phone or other electronic device, an alert should be generated and sent to the child's caregiver. This caregiver could be a Community Health Worker, a village elder, or a sub-village chairman.

X.4.2.2.2 Care Reminder Process Flow

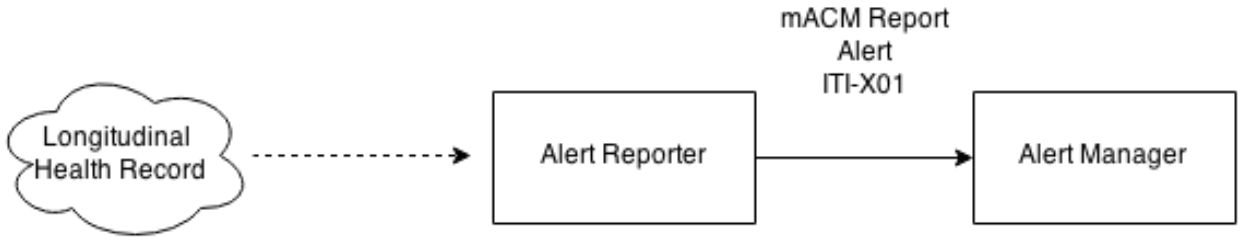


Figure X.4.2.2.2-1: Care Reminders

X.5 mACM Security Considerations

The implementer of this profile is advised that many risks cannot be mitigated by the IHE profile and instead the responsibility for mitigation is transferred to the vendor, and occasionally to the operational environment.

For security considerations on transactions between the Alert Manager and Alert Consumer Actors, implementers should adopt those defined in PCD.

To address identified security risks for the transactions defined in this profile between the Alert Reporter and the Alert Manger, implementers should ensure that:

- All actors in mACM should be grouped with a Consistent Time (CT) Profile - Time Client Actor. This grouping will assure that all systems have a consistent time clock to assure a consistent timestamp for audit logging and alert dissemination.
- All actors in mACM should be grouped with an Audit Trail and Node Authentication (ATNA) Profile - Secure Node Actor or ATNA Secure Application Actor. This grouping will assure that only highly trusted systems can communicate and that all changes are recorded in the audit log.
- All actors in mACM should be grouped with an IUA Actor as appropriate. This grouping will enable service side access control and more detailed audit logging.
- All actors in mACM should be grouped with the appropriate actor from the Enterprise User Authentication (EUA) Profile to enable single sign-on inside an enterprise by facilitating one name per user for participating devices and software.

In particular, appropriate care should be taken when a subject of care is identified in the alert as the content may contain PHI. There are many security and privacy concerns with mobile devices, including lack of physical control. Many common information technology uses of HTTP, including REST, are accessing far less sensitive information than health documents. These factors present an especially difficult challenge for the security model. It is recommended that application developers perform a Risk Assessment in the design of the applications, and that operational environment using mACM perform Risk Assessments in the design and deployment of the operational environment.

An Alert Manager should not return any patient information unless proper authentication and communications security have been proven.

There are many reasonable methods of securing interoperability transactions. These security models can be layered in without modifying the characteristics of the mACM Profile transactions. The use of TLS is encouraged, specifically the use of the ATNA Profile. User authentication on mobile devices is encouraged using Internet User Authorization (IUA) Profile. The network communication security and user authentication are layered in at the HTTP transport layer and do not modify the interoperability characteristics defined in the mACM Profile.

X.5.1 Patient Safety Considerations

If used beyond original use cases, patient safety risks may need to be assessed.

X.6 mACM Cross Profile Considerations

X.6.1 Health Worker Directory Services

The Alert Reporter Actor would receive great benefit in the context of a health care network that has a health worker. These registries can be used to create a list of enterprise IDs for health workers. Such a service for health workers could be provided, for example, by the:

- InfoManager Actor in the Care Services Discovery (CSD) Profile
- Directory Actor in the Healthcare Provider Directory (HPD) Profile
- Directory Actor in the Personnel White Pages (PWP) Profile

Though the manner in which these, or other similar directory services, are queried is not prescribed by this profile. Example interaction diagrams illustrating the utility of such a services are provided in Figure X.6.1-1 and Figure X.6.1-2.

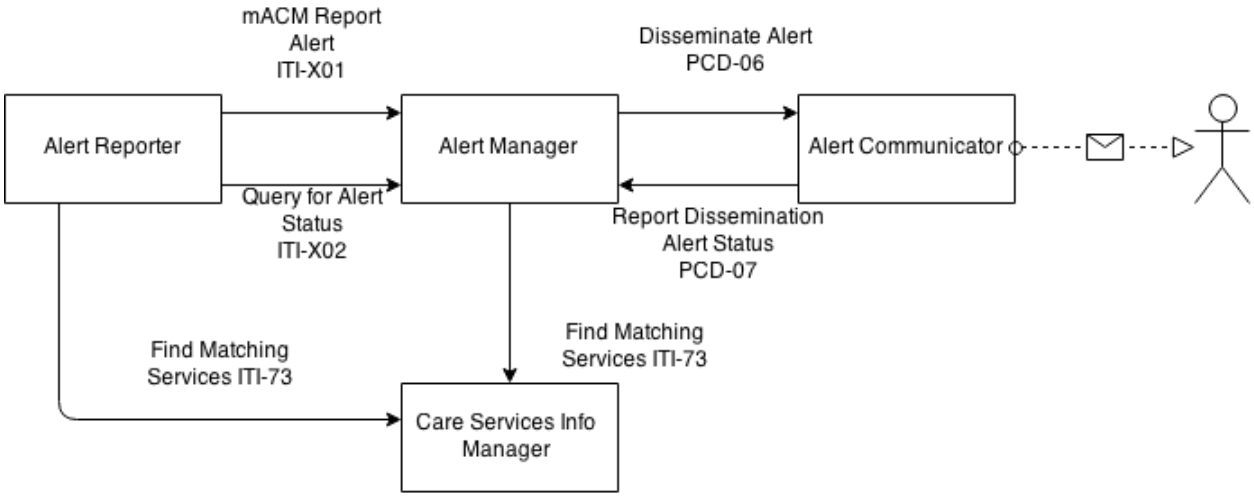


Figure X.6.1-1: mACM Actor Interactions with a Health Worker Registry

In Figure X.6.1-1 the CSD Info Manager Actor acts as a directory of health workers in the health system. The Alert Reporter executes an appropriate Find Matching Services ITI-73 transaction to determine a list of enterprise IDs for targeted health workers according to internal business requirements. The Alert Reporter then sends the alert on to the Alert Manager using the Report Alert – Mobile Device Option transaction. The Alert Manager may also execute an appropriate Find Matching Services ITI-73 transaction in order to determine the contact points (e.g., cell phone number) of the referenced health worker.

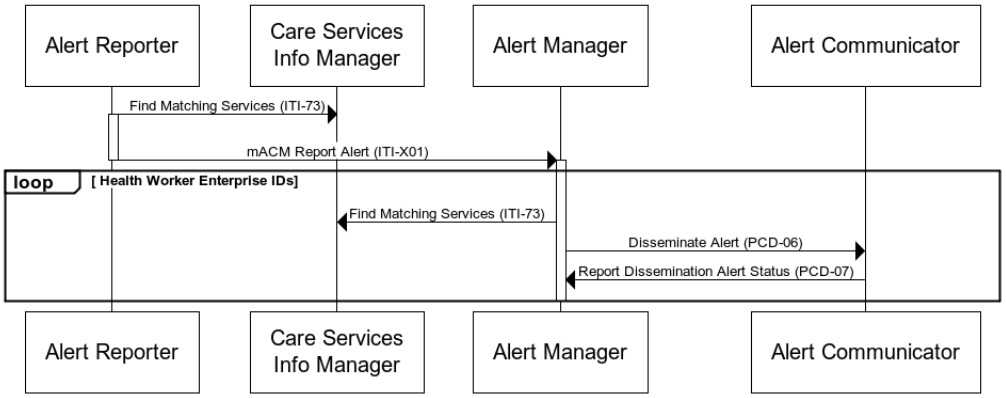


Figure X.6.1-2: Sequencing of mACM Actor Interactions with a Health Worker Registry

In Figure X.6.1-2 a potential sequencing of the transactions in Figure X.6.1-1 is illustrated. These steps may be described as follows:

1. The Alert Report executes ITI-73 against a Care Services Info Manager to determine the enterprise IDs for a list of Health Workers matching a set of criteria appropriate the alert it is reporting. The specific criteria used are context dependent on the business reason for the alert.
2. Using the resultant list of Health Worker enterprise IDs, the Alert Report executes ITI-X01 to report the given alert to an Alert Manager.
3. For each Health Worker identified in the alert, the Alert Manager determines available contact points (e.g., telephone number, email address) by executing ITI-73 against a Care Services Info Manager. The Alert Manager may optimize for network performance by caching the results of the ITI-73 transactions.
4. The Alert Manager disseminates the alert to an Alert Communicator using PCD-06.
5. The Alert Communicator reports back status information using PCD-07.

X.6.2 Client Registry Services

The Alert Reporter Actor would receive great benefit in the context of a health care network that has a health a client registry. These registries can be used to create a list of enterprise IDs for subjects of care. Such a service for a client registry could be provided, for example, by the:

- The Patient Demographics Supplier Actor in the Patient Demographics Query (PDQ) Profile
- The Patient Demographics Supplier Actor in the Patient Demographics Query for Mobile (PDQm) Profile

Though the manner in which these, or other similar directory services, are queried is not prescribed by this profile, example interaction diagrams illustrating the utility of such a services are provided in Figure X.6.2-1 and Figure X.6.2-2.

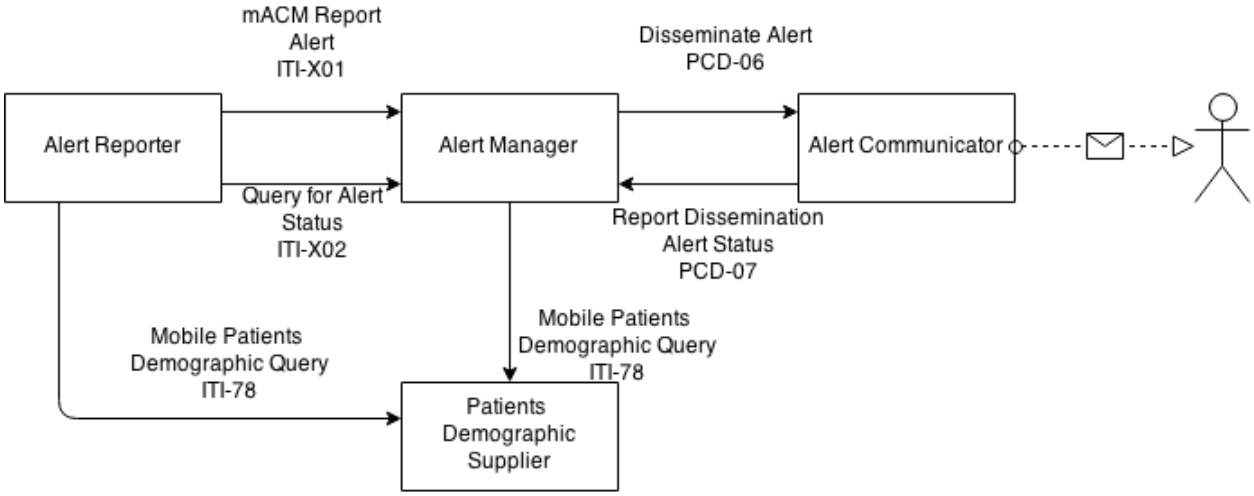


Figure X.6.2-1: mACM Actor Interactions with a Client Registry

In Figure X.6.2-2 the PDQ(m) Patient Demographics Supplier Actor acts as a directory of subjects of care in the health system. The Notification Publisher executes an appropriate Mobile Patients Demographic Query ITI-78 transaction to determine a list of enterprise IDs for targeted subjects of care according to internal business requirements. The Alert Reporter then sends the alert on to the Alert Manager using the Report Alert – Mobile Device Option transaction. The Alert Manager may also execute an appropriate Mobile Patients Demographic Query ITI-78 transaction in order to determine the contact points (e.g., cell phone number) of the referenced subject of care.

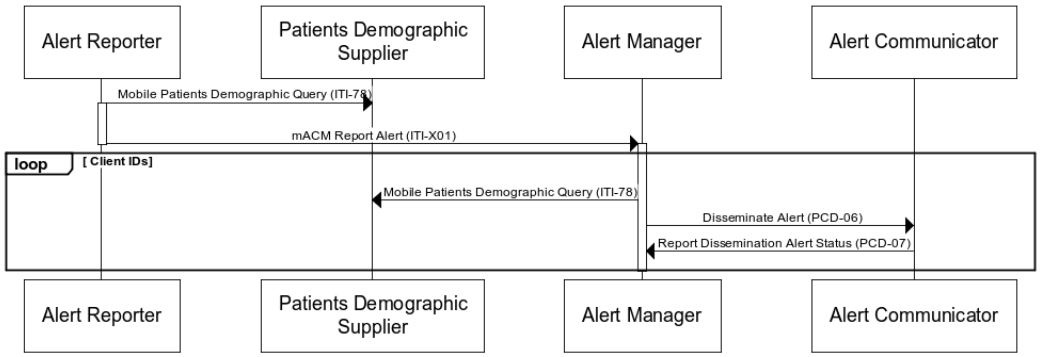


Figure X.6.2-2: Sequencing of mACM Actor Interactions with a Client Registry

In Figure X.6.2-2 a potential sequencing of the transactions in Figure X.6.2-1 is illustrated. These steps may be described as follows:

1. The Alert Report executes ITI-78 against a Patient Demographics Supplier to determine the enterprise IDs for a list of Subjects of Care matching a set of criteria appropriate the alert it is reporting. The specific criteria used are context dependent on the business reason for the alert.
2. Using the resultant list of Subject of Care enterprise IDs, the Alert Report executes ITI-X01 to report the given alert to an Alert Manager.
3. For each Subject of Care identified in the alert, the Alert Manager determines available contact points (e.g., telephone number, email address) by executing ITI-78 against a Patient Demographics Supplier. The Alert Manager may optimize for network performance by caching the results of the ITI-78 transactions.
4. The Alert Manager disseminates the alert to an Alert Communicator using PCD-06.
5. The Alert Communicator reports back status information using PCD-07.

Volume 2 – Transactions

3.X01 Mobile Report Alert [ITI-X01]

3.X01.1 Scope

The Mobile Report Alert transaction is used to issue alerts to health workers and subjects of care.

An Alert Reporter initiates a Mobile Report Alert transaction against an Alert Manager.

3.X01.2 Actor Roles

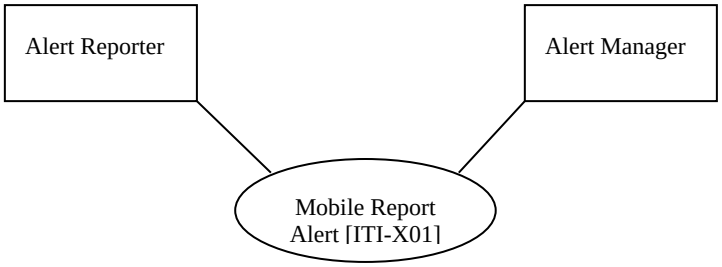


Figure 3.X01.2-1: Use Case Diagram

Table 3.X01.2-1: Actor Roles

Actor:	Alert Reporter
Role:	Sends an alert to an Alert Manager for dissemination to a health worker or subject of care.
Actor:	Alert Manager
Role:	Accepts an alert from an Alert Reporter for dissemination to subjects of care and health workers

3.X01.3 Referenced Standards

- FHIR® DSTU v2 http://hl7.org/fhir/2015May/index.html
- HL7® - Health Level 7 Version 2.6 Ch7 Observation Reporting
- ISO/IEEE 11073-10201 Domain Information Model
- ISO/IEEE 11073-10101 Nomenclature
- JSON RFC 7159

- XML
- HTTP 1.1
- XML Schema 1.1
- RFC 5646 Tags for Identifying Languages

3.X01.4 Interaction Diagram

The following interaction diagram illustrates an Alert Reporter sending a Mobile Report Alert to an Alert Manager via the message semantics as defined for a `Flag` resource.

3.X01.4.1 Mobile Report Alert Request

The Alert Manger shall support the message semantics for create, update and read as defined in 2.1.0.1.8, 2.1.0.10, 2.1.0.13 of FHIR® DSTU v2 as applicable to a Flag resource defined in 5.2.

The `Flag` resource is furthered constrained as defined in Section 3.X01.4.1.2.1.

3.X01.4.1.1 Trigger Events

An Alert Reporter triggers a Mobile Report Alert Request according to the business rules for the alert being issued. These business rules are out of scope of this profile.

3.X01.4.1.2 Message Semantics

An Alert Reporter initiates a create request as defined in 2.1.0.13 of FHIR® DSTU v2 on the `Flag` resource in order to report a new alert.

An Alert Manager shall support receiving a request in both the JSON and the XML messaging formats as defined in FHIR® DSTU v2. An Alert Reporter shall use either the XML or the JSON messaging formats as defined in FHIR® DSTU v2.

3.X01.4.1.2.1 FHIR® Flag Constraints

An Alert Manger and an Alert Reporter that support he Query for Alert Status transaction shall
620 transaction shall use a FHIR® `Flag` resource as constrained Table 3.X01.4.1.2.1-1. The Data Field column in Table 3.X01.4.1.2.1-1 references the object model defined in 5.20.3 of FHIR® DSTU v2.

The base URL:

http://www.ihe.net/fake_url_for_public_comment/mACM/Profile

625 shall be prepended onto relative portion of the *`url`* attribute for the extension points defined in Table 3.X01.4.1.2.1-1 and Table 3.X01.4.1.2.1-2.

Table 3.X01.4.1.2.1-1: Flag Resource Constraints

Data Field & Cardinality	Description & Constraints	FHIR® Data Type
`category` `[1..1]`	Signifies that this flag is intended to be disseminated by the Alert Manager according to the expected actions defined in 3.X01.4.1.3. This data field is defined as an extension constrained so that: • The value "`urn:ihe:iti:2015:macm` "is stored in `coding.code` attribute • the value "`1.3.6.1.4.1.19376.1.2.5.1`" is stored in the `coding.system` attribute	`CodableConcept`
`extension` `[1..*]`	This data field specified one or more means to identify an alert recipient as an extension point. This data field is defined as an extension constrained so that: • the `url` attribute has relative value "`flag.recipient`" • it contains Alert Recipient sub-extensions as defined in Table 3.X01.4.1.2.1-2	`extension`
`lastUpdated` `[1..1]`	The last time that the Alert resource was updated or an alert dissemination status was updated. Note that this cardinality differs from the cardinality required in the FHIR® base resource.	`instant`
`code` `[1..1]`	The alert content. This data field is constrained so that: • there shall be unstructured text in the `text` attribute • the alert should also be coded according a jurisdiction defined code system, for example ISO/IEEE 11073-10101 (Block E).	`CodableConcept`

Data Field & Cardinality	Description & Constraints	FHIR® Data Type
`extension [0..*]`	This data field contains enriched media representation of the alert message, such as a voice recording. This may be used, for example for compliance with jurisdictional accessibility requirements, literacy issues, or translations of the unstructured text content in other languages. This data field is defined as an extension constrained so that: • the `url` attribute has relative value "`flag.media`" • a valid reference to or encoding of the media content stored in `valueAttachment` with the `language` and `contentType` attributes specified if known	`Attachment`
`extension [1..1]`	This data field identifies the priority of the alert, for example the Alert Priority flags column in IHE PCD TF-2: Table B.8-4. This data field is defined as an extension constrained so that: • the `url` attribute has relative value "`flag.priority`" • a valid priority code stored in `valueCodableConcept`.	`CodableConcept`
`extension [0..*]`	This data field identifies secondary characteristics of the alert, for example the abnormality flags IHE PCD TF-2: Table B.8-3. This data field is defined as an extension constrained so that: • the `url` attribute has relative value "`flag.characteristic`" • a valid status code is stored in `valueCodableConcept`.	`CodableConcept`

630 **Table 3.X01.4.1.2.1-2: Alert Recipient Extension**

Data Field & Cardinality	Description & Constraints	FHIR® Data Type
`extension [0..*]`	This data field specifies a means to identify an alert recipient. This data field is defined as an extension constrained so that: • the `url` attribute has relative value "`flag.recipient.identifier`" • an enterprise identifier of a health worker, subject of care, or designated caregiver is stored in `valueIdentifier`	`Identifier`

Data Field & Cardinality	Description & Constraints	FHIR® Data Type
`extension [0..*]`	This data field specifies a means to identify an alert recipient by contact information such as a telephone number, fax or email address. This data field is defined as an extension constrained so that: • the `url` attribute has relative value "`flag.recipient.contactPoint`" • a valid means of contact is stored in `valueContactPoint.`	`ContactPoint`
`extension [0..*]`	This data field specified one or more means to identify an alert recipient as a health worker. This data field is defined as an extension constrained so that: • the `url` attribute has relative value "`flag.recipient.practitioner`" • a valid reference to a `Practitioner` resource is stored in `valueReference`.	`Reference( Practitioner )`
`extension [0..*]`	This data field specified one or more means to identify an alert recipient as a subject of care. This data field is defined as an extension constrained so that: • the `url` attribute has relative value "`flag.recipient.patient`" • a valid reference to a `Patient` resource is stored in `valueReference.`	`Reference ( Patient )`
`extension [0..*]`	This data field specified one or more means to identify an alert recipient as a set of health workers (such as a care group or a geographic selection). The group may also represent subjects of care, for example a cohort of patients. This data field is defined as an extension constrained so that: • the `url` attribute has relative value "`flag.recipient.group`" • a valid reference to a `Group` resource stored in `valueReference`	`Reference ( Group )`

3.X01.4.1.3 Expected Actions

The Alert Manager shall issue a Mobile Report Alert Response upon receipt of a Mobile Report Alert Request.

635 If the Mobile Report Alert Request was valid and identified recipients within the jurisdiction of the Alert Manager, then the Alert Manager shall disseminate the alert to designated recipients according to the PCD-06 Disseminate Alert transaction. The Alert Manager shall record dissemination status updates related to the dissemination of the alert. The jurisdiction should determine the retention policy for dissemination status events.

There are no expected actions on the Alert Reporter upon acknowledgement (or lack thereof) of the successful creation or update of the alert.

If the Alert Communicator initiates a Report Dissemination Alert Status PCD-07 transaction, then it should encode the status of this alert dissemination according to the "future assignment" column in IHE PCD TF-2: Table B.8-2. This value shall be stored in the extension point defined in Table 3.X02.4.1.2.1-2 for the relative URL "`flag.dissemination.code`". This extension point shall be constrained so that the future assignment status is stored in the `code` attribute of the coding field.

3.X01.4.2 Mobile Report Alert Response

The Mobile Report Alert transaction uses the response semantics as appropriate according to the FHIR® transaction initiated by the Alert Reporter. Specific semantics are defined in 2.1.0.10 and 2.1.0.13 in FHIR® DSTU v2 for the `Flag` resource, as defined in 5.20.

The `Flag` resource is furthered constrained as defined in Section 3.X01.4.1.2.1.

3.X01.4.2.1 Trigger Events

An Alert Manager issues a Mobile Report Alert Response upon receipt of a Mobile Report Alert Request.

3.X01.4.2.2 Message Semantics

The Alert Manger shall respond with the appropriate response codes as defined in 2.1.0.10 and 2.1.0.13 in FHIR® DSTU v2.

3.X01.4.2.3 Expected Actions

There are no expected actions on the Alert Reporter upon receipt (or lack thereof) of the Mobile Report Alert Response.

There are no expected actions on the Alert Manager upon delivery of the Mobile Report Alert Response.

3.X01.5 Security Considerations

See the security considerations defined in IHE ITI TF-1:X.5.

In addition, appropriate precautions should be taken against Denial of Service attacks or spam when the Alert Manager is exposed outside of a data center.

3.X01.5.1 Security Audit Considerations

The ATNA logging policy is defined by the implementing jurisdiction taking into account the implementation context.

3.X02 Query for Alert Status [ITI-X02]

3.X02.1 Scope

This transaction is used by an Alert Reporter to determine from the Alert Manager the status and any acknowledgements of one or more alerts by the recipient.

3.X02.2 Actor Roles

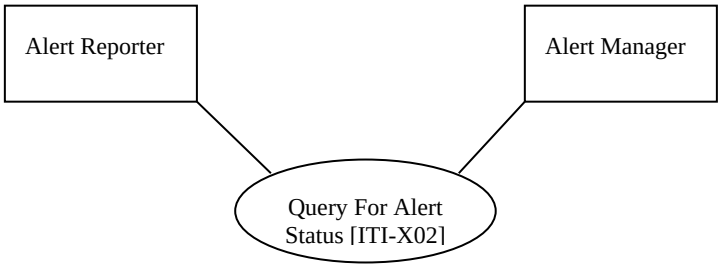


Figure 3.X02.2-1: Use Case Diagram

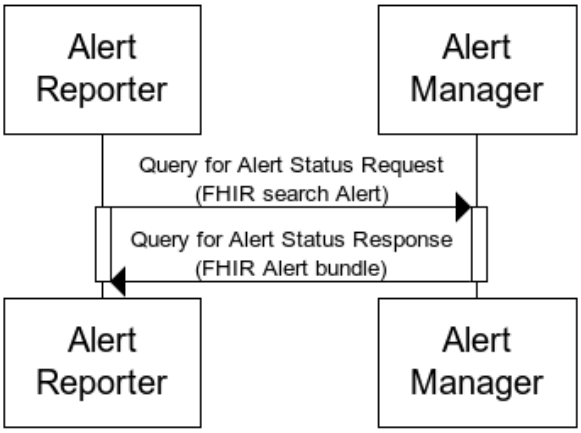
Table 3.X02.2-1: Actor Roles

Actor:	Alert Reporter
Role:	Queries an Alert Manager for the status of one or more alerts that it issued.
Actor:	Alert Manager
Role:	Sends any status messages and human recipient acknowledgments for the indicated alerts

3.X02.3 Referenced Standards

- FHIR® DSTU v2 http://hl7.org/fhir/2015May/index.html
- HL7® - Health Level 7 Version 2.6 Ch7 Observation Reporting
- ISO/IEEE 11073-10201 Domain Information Model
- ISO/IEEE 11073-10101 Nomenclature
- World Geodetic System WGS-84
- JSON RFC 7159
- XML
- HTTP 1.1
- XML Schema 1.1

3.X02.4 Interaction Diagram



3.X02.4.1 Query for Alert Status Request

The Alert Manager shall support the search request message as defined in 2.1.0.14 in FHIR® DSTU v2 on the `Flag` resource, defined in 5.20.

The `Flag` resource is furthered constrained as defined in Sections 3.X01.4.1.2.1 and 3.X02.4.1.2.1.

3.X02.4.1.1 Trigger Events

An Alert Reporter triggers a Query for Alert Status Request according to the business rules for the alert(s) being investigated. These business rules are out of scope of this profile.

3.X02.4.1.2 Message Semantics

An Alert Reporter initiates a search request as defined in 2.1.0.14 of FHIR® DSTU v2 on the `Flag` resource as constrained in Sections 3.X01.4.1.2.1 and 3.X02.4.1.2.1.

An Alert Manager shall support combinations of search parameters through ANDing and ORing as defined in FHIR®'s "2.1.1.3.13 Composite Search Parameters."

An Alert Manager shall support searching against the following search parameters:

- `flag._id`
- `flag.identifier`
- `flag.patient`
- `flag.recipient._id*`
- `flag.recipient.identifier*`
- `flag.category`
- `flag._lastUpdated`

- `flag.period`
- `flag.code`
- `flag.priority`*
- `flag.characteristic`*
- `flag.dissemination`*
- `flag.dissemination.timestamp`*
- `flag.dissemination.location`*
- `flag.dissemination.recipient`*

* Note that this search parameter is on an extension element. See FHIR® DSTU v2 6.19.5 for more details.

An Alert Manager shall support receiving a request in both the JSON and the XML messaging formats as defined in FHIR® DSTU v2. An Alert Reporter shall use either the XML or the JSON messaging formats as defined in FHIR® DSTU v2.

3.X02.4.1.2.1 FHIR® Flag Constraints

An Alert Manger and an Alert Reporter that supports the Query for Alert Status transaction shall use a FHIR® `Flag` resource with zero or more dissemination status extension in Table 3.X02.4.1.2.1-1.

The dissemination status extension shall contain the sub-extensions as described in Table 3.X02.4.1.2.1-2.

The Alert Manager should provide an extension definition for the dissemination status extension that includes the fields defined in Table 3.X02.4.1.2.1-2 and 3.X02.4.1.2.1-3 and as specified in 1.16.10 of FHIR® DSTU v2.

The base URL:

http://www.ihe.net/fake_url_for_public_comment/mACM/Profile

shall be prepended onto the relative portion to the `url` attribute for the extension points defined in Table 3.X02.4.1.2.1-1, Table 3.X02.4.1.2.1-2 and Table 3.X02.4.1.2.1-3.

Table 3.X02.4.1.2.1-1: Flag Resource Constraints

Data Field & Cardinality	Description & Constraints	FHIR® Data Type

Data Field & Cardinality	Description & Constraints	FHIR® Data Type
`extension [0..*]`	The extension point for the dissemination status resource. This data field is defined as an extension constrained so that: • the `url` attribute has relative value "`flag.dissemination`" • it contains Dissemination Status sub-extensions as defined in Table 3.X02.4.1.2.1-2	`extension`

Table 3.X02.4.1.2.1-2: Dissemination Status Extension

Data Field & Cardinality	Description & Constraints	FHIR® Data Type
`extension [1..1]`	This data field specified one or more means to identify an alert recipient for which this dissemination status event is referencing. This data field is defined as an extension constrained so that: • the `url` attribute has relative value "`flag.dissemination.recipient`" • it contains Dissemination Status Recipient sub-extensions as defined in Table 3.X02.4.1.2.1-3	`extension`
`extension [1..1]`	The time at which a dissemination status was generated by the Alert Communicator or upon which the recipient responded with a unstructured text message. This data field is defined as an extension constrained so that: • the `url` attribute has relative value "`flag.dissemination.timestamp`" • a timestamp stored in `valueInstant`.	`instant`
`extension [0..*]`	Indicates a dissemination status of the alert. This data field is defined as an extension constrained so that: • the `url` attribute has relative value "`flag.dissemination.code`" • a valid status code is stored in `valueCodableConcept` • if there is unstructured text content associated to the dissemination event, this shall be stored in the `code.text` element	`CodableConcept`
`extension [0..1]`	An extension point for location information for a dissemination status event. This data field is defined as an extension constrained so that: • the `url` attribute has relative value "`flag.dissemination.location`" • a valid location, if known, is stored in `valueLocation`	`location`

745 **Table 3.X02.4.1.2.1-3: Dissemination Status Recipient Extension**

Data Field & Cardinality	Description & Constraints	FHIR® Data Type
`extension [0..*]`	This data field specifies a means to identify an alert recipient. This data field is defined as an extension constrained so that: • the `url` attribute has relative value "`flag.recipient.identifier`" • an enterprise identifier of a health worker, subject of care, or designated caregiver is stored in `valueIdentifier`	`Identifier`
`extension [0..*]`	This data field specifies a means to identify an alert recipient by contact information such as a telephone number, fax or email address. This data field is defined as an extension constrained so that: • the `url` attribute has relative value "`flag.recipient.contactPoint`" • a valid means of contact is stored in `valueContactPoint.value`	`ContactPoint`
`extension [0..*]`	This data field specifies one or more means to identify an alert recipient as a health worker. This data field is defined as an extension constrained so that: • the `url` attribute has relative value "`flag.recipient.practitioner`" • a valid reference to a `Practitioner` resource is stored in `valueReference`	`Reference( Practitioner )`
`extension [0..*]`	This data field specifies one or more means to identify an alert recipient as a subject of care. This data field is defined as an extension constrained so that: • `url` attribute has relative value "`flag.recipient.patient`" • a valid reference to a `Patient` resource is stored in `valueReference`	`Reference ( Patient )`

3.X02.4.1.3 Expected Actions

Upon receipt of a valid Query for Alert Status Request from an Alert Reporter, an Alert Manager shall:

750
- Determine if there are any alerts matching the request
- Send a Query for Alert Status Response to the Alert Reporter

3.X02.4.2 Query for Alert Status Response

The Query for Alert Status transaction uses the response semantics as appropriate according to the search response message as defined in 2.1.0.14 of FHIR® DSTU v2 as applicable for the `Flag` resource, as defined in 5.20.

The `Flag` resource is furthered constrained as defined in Sections 3.X01.4.12.1 and 3.X02.4.12.1.

3.X02.4.2.1 Trigger Events

The Alert Manager sends the Query for Alert Status Response to the Alert Reporter upon receipt of a Query for Alert Status Request.

3.X02.4.2.2 Message Semantics

The Alert Manager shall support the search response message as defined in 2.1.0.14 in FHIR® DSTU v2 on the `Flag` resource, defined in 5.20.

The `Flag` resource is furthered constrained as defined in Sections 3.X01.4.1.2.1 and 3.X02.4.1.2.1.

3.X02.4.2.2.1 Bundle Pagination

If an Alert Manager wishes to page query results, then it shall do so as defined in 2.1.0.19 of FHIR® DSTU v2. In this case, the Alert Manager shall provide the `first` and `next` navigation links.

3.X02.4.2.3 Expected Actions

There are no expected actions on the Alert Reporter upon receipt of the Query for Alert Status Response.

3.X02.5 Security Considerations

See the security considerations defined in X.5.

3.X02.5.1 Security Audit Considerations

The ATNA logging policy is defined by the implementing jurisdiction taking into account the implementation context.

Volume 2 Namespace Additions

Add the following terms to the IHE General Introduction Appendix G:

The mACM Profile defines following OIDs:

- 1.3.6.1.4.1.19376.1.2.5 the root OID for the mACM Profile

- 1.3.6.1.4.1.19376.1.2.5.1 the OID for the code set used by mACM for specifying the category of a FHIR® flag resource

