Integrating the Healthcare Enterprise

IHE Patient Care Device (PCD) White Paper

MEM Remote Device Command (RDC)

Rev. 1.1 – Published

Date: October 23, 2018

Author: IHE PCD Technical Committee

Email: pcd@ihe.net

Please verify you have the most recent version of this document. See here for Published versions and here for Public Comment versions.

Foreword

This white paper is published on October 23, 2018. Comments are invited and can be submitted at http://www.ihe.net/PCD_Public_Comments.

General information about IHE can be found at www.ihe.net.

Information about the IHE Patient Care Device domain can be found at 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 Patient Care Device Technical Framework can be found at http://www.ihe.net/Technical_Frameworks.

CONTENTS

Introduction 4
1 Purpose 4
2 Goals 4
3 Non-Goals 4
4 Use Cases 4
5 Scope 5
6 Not in Scope 6
7 Constraints 6
8 Deliverables 6
9 Definitions 6
10 References 8
11 IHE Profiles 8
12 IHE Profile Actors 8
13 IHE PCD Transactions 9
14 Safety and Security 10
15 What we have 10
16 What we need 10
17 RDC Actors and Transactions 15
18 Remote Device Command Request 16
19 Message Content for Specific Use Cases 20
20 Futures 24

Introduction

Organization – Integrating the Healthcare Enterprise (IHE)

Domain – Patient Care Device (PCD)

Working Group – Medical Equipment Management (MEM)

Profile – Device Management and Communication (DMC)

Project – Remote Device Command (DMC)

Lead – Monroe Pattillo (IHE PCD PC co-chair) – Practical Health Interoperability, LLC

Date – 2018-10-23

1 Purpose

The purpose of this IHE PCD MEM Working Group activity is to identify a means for communicating medical device command requests and responses in a uniform and device type independent manner.

2 Goals

The primary goal is to define a solution for a constrained number of use case specific commands and any associated responses to specific types of medical devices in a uniform and device type independent manner.

3 Non-Goals

Creating a normative standard for device remote command communication is not a goal.

Creating a single solution for all possible use cases of medical device remote commands is not a goal.

4 Use Cases

The following are the defined use cases for this working group effort. The means of communicating medical device remote command and responses is the same across all of the listed use cases.

- Use Case #1 – Temporarily silencing the audio of an active alert given the reception of the alert as context (doesn't clear the active alert) – example: Clinician receives alert notification and has accepted it, or is on way to room, or enters room, temporarily silence alert audio while clinician resolves the alert. Any person or system with the appropriate context and authority could issue the command. This capability is not exclusive to the clinician that receives the alert. For example, a Medical Equipment Management Location Services (MEMLS) consumer can detect the clinician entering the patient room and can currently signal a nurse call system to change dome light status. It could also temporarily silence an alert as the clinician is detected entering the patient room, providing it is the appropriate clinician (any clinician, any clinician in that unit, or only the clinician currently assigned to the patient). The change in the inactivation state of the active alert resulting from the processing of this command by the target device would be expected to result in the sending of an ACM PCD-04 message to communicate the change in inactivation state. An ACM Alarm Manager (AM) could use this signal to end escalation. Risk analysis would need to be done before the capability would be engaged once implemented.

- Use Case #2 – Clear the device displayed volume infused so far for documentation purposes based upon access to the infusion order (doesn't affect active program) – example: Reset of displayed infused so far creates a documentation checkpoint for recording by clinicians. For multiple infuser pumps the requestor would need to indicate a specific infuser. This may be implicit in the identification of the infusion order. The processing of this command prior to clearing the volume infused so far would be expected to result in an Infusion Pump Event Communication (IPEC) Profile Device Observation Reporter (DOR) sending an infusion update observation and a Device Enterprise Communication (DEC) Profile Device Observation Reporter sending a device observation message. These messages would indicate the volume infused so far prior to reset and could be used for patient infusion record updating. This would considerably reduce clinician efforts in this regard as well as improving recording accuracy and timeliness. This capability would permit a user interface to be developed to select the multiple pumps associated with one or more patients and to record their volume infused so far and to have them reset. Support for a single RDC command to clear the infusers of multiple pumps across one or more patients or the multiple infusers of a single pump in a single command is not supported.
- Use Case #3 – Remote unlock of a device operator panel. Would revolve around automation; either clinician with security unlocks remotely or authorized user of EMR, through normal usage of the software, triggers message from the EMR to the device to unlock the panel for use. The motivation would be to remove the burden of a clinician having to remember unlock codes for a variety of device manufacturers, types, and models by storing that in another system to which the clinician has approved access. That system would be commanded to unlock a specific device. The device may have multiple unlock levels. Both the level and the code would need to be provided. Risk analysis would need to be done before the capability would be engaged once implemented.

5 Scope

For the IHE current development cycle the scope is narrowed to small set of noncontroversial achievable use cases so as to achieve an initial end result of pre-qualification testing over the Internet either virtually using interactive systems or through the exchange of message texts with the anticipated end result being selected as an IHE PCD New Directions demonstration at the HIMSS 2018 North America Interoperability Showcase (Las Vegas, NV) or later at the AAMI 2018 Interoperability Experience demonstration (Long Beach, CA). As there is no expectation of a Trial Implementation (TI) profile in time for the 2018 Pre-Connectathon, there is no expectation of profile verification at the 2018 IHE North America Connectathon.

6 Not in Scope

This effort knowingly does not encompass all medical device remote command use cases or functions.

This effort knowingly does not encompass data responses which are sufficiently voluminous so as to require pagination.

While this white paper identifies numerous data items that may be requisite for security validation the configuration loading, maintenance, and utilization of databases (SQL, LDAP, etc.) of such items is outside the scope of this white paper.

7 Constraints

Compromises are required to achieve a New Directions demonstration in a limited time frame with limited modification of existing equipment hardware and software implementations. These compromises should be clearly identified in demonstrations.

Avoid identification of the constrained implementation as normative (industry standards approved).

8 Deliverables

The following are the deliverables of this effort.

- This white paper on project definition and use of PCD messaging to communicate the medical device remote command and response messages
- Separately, not as a part of this white paper, sample HL7®[1] v2.6 message content resulting from demonstrations of this capability. This information could be used as message examples within a PCD profile supplement.

9 Definitions

These are the definitions outside the normal IHE and IHE PCD set of definitions

CMMS – Computerized Maintenance Management System

DMC – Device Management Communication

DMIC – Device Management Information Consumer, from the PCD Medical Equipment Management Device Management Communication Profile

DMIO – Device Management Information Observation transaction, from the PCD Medical Equipment Management Device Management Communication Profile

[1] HL7 is the registered trademark of Health Level Seven International.

DMIR – Device Management Information Reporter, from the PCD Medical Equipment Management Device Management Communication Profile

MEM – Medical Equipment Management

10 References

The current version of the PCD Medical Equipment Management Device Management Communication Profile and the PCD Technical Framework can be found at http://ihe.net/Technical_Frameworks/#pcd

Where practicable, this effort makes use of IEEE 11073 prior efforts and attempts to identify any need for changes to those efforts.

Standards

- HL7 v2.6 with forward looking references to Participate (PRT) segment
- IEEE 11073-10201 and IEEE 11073-10101a

11 IHE Profiles

The following IHE PCD profiles were utilized.

- Medical Equipment Management Device Management Communication

It has been recommended that this effort should be recognized as a new and unique Medical Equipment Management Profile. To that end, as of 26 Aug 2016 the IHE profile name and acronym Remote Device Command (RDC) is unique to the IHE profiles and acronyms list at this location.

http://wiki.ihe.net/index.php/Profiles

Going forward this effort and its deliverables, including the potential new profile, will be referred to as Remote Device Command (RDC).

12 IHE Profile Actors

The following PCD Medical Equipment Management Device Management Communication Profile actors are referenced.

- Device Management Information Reporter (DMIR)
- Device Management Information Consumer (DMIC)

The following new actors were identified for use in this document and for possible inclusion in a future profile or for changes to the Medical Equipment Management Device Management Communication Profile. The names and acronyms have not been validated for IHE-wide uniqueness as of 03 Sep 2016.

- Remote Device Command Client (RDCC) refers to IHE actors sending commands. This may be a device or a gateway.
- Remote Device Command Server (RDCS) refers to IHE actors responding to commands. This may be a device or a gateway.

13 IHE PCD Transactions

Data items from existing listed PCD transactions could potentially be referenced as contextual identification and access data items in commands.

- Device Observation [PCD-01]
- Infusion Order [PCD-03]
- Report Alert [PCD-04]
- Infusion Event [PCD-10]
- Device Management Information Observation [PCD-15]

The following new transactions were identified for use in this document and for possible inclusion in a future profile. The name and acronym have not been validated for IHE-wide uniqueness.

- Remote Device Command Request (RDCRQ) (sent from RDCC to RDCS) [PCD-17]
- Remote Device Command Response (RDCRS) (sent from RDCS to RDCC) [PCD-18

It is assumed that an HL7 ACK (Accept, not Application) while being sufficient as confirmation of receipt of the command and of acceptance of the values in the request it would not be sufficient to communicate command response data or to signal completion of a command with significant time to complete requested actions, such as mechanical movements. The ACK is expected to go beyond a simple status response and to include in the ERR segment details as to the reason for an error response short of assisting security compromises.

The command response message could also include the prior state or value of the object being changed.

It is assumed that RDCRS would be communicated over the TCP socket session that was initiated by the RDCC and utilized for the sending of the command request to the RDCS. This is assumed so as to permit devices without a TCP port listener to initiate commands to other devices and to receive the response. This minimizes the number of IP routable server destinations which are likely to require static or pseudo-static assigned IP addresses.

It is assumed that data collections sent in response to the command request are sufficiently short so as to allow for a single transaction response to contain all the requested data and not require multiple messages and responses for pagination.

It is assumed that the RDCS can perform any required functional verification and security checks in a reasonably short period of time without operator manual interaction. If the norm of duration for this functionality turns out to be an extended period of time, say potentially upwards of a significant portion of a minute to minutes then an Accept ACK would be returned upon receipt of the command and any immediately processed checks, and the response message would indicate command has been fully processed. Application acknowledgements are not currently required.

The command request is not an inquiry for data to be returned which might require its own set of response or pagination transactions.

14 Safety and Security

General Statements

Given that this makes use of existing PCD profiles, connectivity authentication and data transfer security are as per the PCD Technical Framework understanding between the ITI and the PCD domains.

This white paper was developed with the awareness and review of the PCD MEM Cyber Security Working Group.

Specific to this white paper

Device anonymity is one aspect to provide a minimal level of patient safety and device security. If you don't know you shouldn't be permitted to purposefully affect. There are collectively few query systems that would provide all the prerequisite information. Therefore the commanding system would need context, such as an observation, an active alert, or an infusion order and the identification of the system to be commanded (Receiving Application, Receiving Facility, MDS, VMD, device ID, and for multiple infusate pumps the infusate source).

Any command would be constrained by the defined limits of the device or drug library. Physiologic monitors may not have limit min/max parameters which can't be exceeded. In the absence of a privilege code a device without defined ceiling and floor limits on a parameter would not be in consideration for remote parameter adjustment due to patient safety risk.

A single command request is directed at a single device to be commanded.

A single request contains only a single command for a single device.

Multiple parameters should be alterable by a single command.

Multiple commands to a single device are initiated through multiple requests.

Command of a collection of devices is initiated through multiple requests, one per device per request. This assures that the command requestor is aware of the identification and context of all devices being commanded.

15 What we have

We can reuse prior message contextual identification in transport connection definitions, message headers, transaction controls, and observations. This information can be used for device identification confirmation as well as request context for security and safety purposes.

Prior art exists within the IEEE 11073 standard for remote command of medical devices, specifically the -10101 Object Model and Nomenclature for the Control Package, namely MDC_MOC_CNTROL_OP_. The material in the standard is primarily meant to address device internal objects. References to internal handles in external message interfaces are to be avoided.

16 What we need

A uniform device type independent means of component within device identification for command requestors is required. It is typical to make use of IEEE 11073 MDS, VMD, and infusate source values in identifying the source of observations. These same attributes can be passed to devices in order to identify the target object within the device. This approach removes the need to utilize device object internal handles in external message interfaces.

Command Source Identification

It is assumed that a single IEEE 11073 DIM MDS object is the source for the command request such that it can be unambiguously identified.

Command Target Identification

Absent such information it is not possible to unambiguously identify the command target within a multiple component device or system. If such information is defaulted in the absence of communicating specific values such ambiguities could increase patient safety risk and so are to be avoided. Therefore requestor awareness of these attributes is presumed in order to command the device. Requiring these items in commands improves device security. A command requestor not well integrated would be less likely to have awareness of these values.

The follow is proposed as extensions to the 11073-10101 Nomenclature (Section A.3.2.5) and 11073-10201 Object Model (Section 6.6) standards.

0^ MDCX_MOC_CNTRL_OP_MDS Control Package Operation target MDS

0^ MDCX_MOC_CNTRL_OP_VMD Control Package Operation target VMD

0^ MDCX_MOC_CNTRL_OP_INFUSATE_SOURCE Control Package Operation target Infuser*

*Applicable to multiple channel infusion systems.

There is also the need to identify a uniform means for the device to which the command is sent to be able to securely and safely identify the command requestor as a trusted source of command of the device.

Another approach could be the use of the OBX-4 hierarchical dotted notation to identify what is to be commanded. Use of OBX-4 should be rigorously obeyed and agreed between the command requestor and the command recipient prior to assuming that use of OBX-4 values is an approach on which to stand. In the absence of such agreements and conformance to them the use of OBX-4 values is not recommended.

Target identification by communications transport and connection information

It is assumed that a single IEEE 11073 DIM MDS object is the destination of the request so that it can be unambiguously identified.

When using TCP/IP based HL7 v2.x transactions the obvious and easy to implement security mechanisms would be the following:

The IP address and listening TCP port number of the command target – if not known then a potential requestor can't command the device. For patient safety reasons broadcasting remote commands across multiple devices in a network or subnet shall not be supported in a single transaction.

The IP address of the command requestor – if not known by the command recipient then the potential requestor may not be able to command the device. This presumes the command recipient is preconfigured with a list of acceptable command requestors. Given the large quantity of devices in a hospital and the quantity of those who have authority to command each device is also a non-trivial quantity this approach has limited effective value due to the substantial effort required for ongoing maintenance of such information across numerous devices.

HL7 Receiving Application (MSH-5) and Receiving Facility (MSH-6) – if not known then the potential requestor shouldn't be able to command the device. This assumes the command recipient validates these values. It is understood that MSH-6 is optional. As broadcasting is not supported the values should be known, even if the value is empty.

HL7 Sending Application (MSH-3) and Sending Facility (MSH-4) – if not known by the command recipient then shouldn't be able to command the device. This assumes the command recipient is preconfigured with a list of acceptable command requestors. It is understood that MSH-4 is optional. As broadcasting is not supported the values should be known, even if the value is empty.

HL7 Equipment Instance Identifier (OBX-18) or Participation Device (PRT-10) – if not known by the potential command requestor then shouldn't be able to command the device. This assumes the command recipient validates these values. It is unlikely that a person requesting the remote device command would know this information. However, the underlying application that initiates the command message could know this information and present it in a selector to the person or could implicitly tie the device identification with the context of an alert or infusion request.

Command Operation Identification

The command requesting client is required to identify to the command receiving server the command operation being requested.

There is IEEE 11073 prior art (in -10101 and -10201) for device internal identification of a command operation being requested. The material in the standard is primarily meant to address device internal objects. References to internal handles in external message interfaces are to be avoided.

MDC_MOC_CNTRL_OP   Control Package Control Operation Operation identification

The IEEE standard defines the identification of the operation as a numeric value specific to the device instance (value of MDC_ATTR_ID_INSTNO). If already defined by a vendor use of these existing values for external interfacing would lead to different device vendor model instance specific values for the same operations across vendors and device types. This is not appropriate for device type agnostic or vendor agnostic by device type identification of the operation being requested. In the absence of harmonized values for operation identification the following table of command request strings is proposed for demonstration purposes specific to the use cases identified in this white paper.

Table 16-1: Command Identification Strings

Command Identification String	UC #	Command Definition
PAUSE_ALERT_AUDIO	1	Temporarily silence audio of an active alert
CLEAR_DISPL_ VOL_INFUSED	2	Clear displayed volume infused so far
UNLOCK_OPER_PANEL	3	Remote unlock device operator panel

The ***Command Identification String*** is passed as a string datatype associated with the observation identified as MDC_MOC_CNTRL_OP.

It is suggested that the IEEE 11073 WG for nomenclature take up this concern and establish nomenclature (naming structure and a starter set of command identification values). Once they are standardized it is recommended that the above be deprecated in favor of CE datatype values.

Target Value Modification

Read-only parameters would obviously not be candidates for remote modification. The parameter must be read/write in order to be remotely modified. Additionally, there could be a layer of security above the parameter definition that indicates whether or not the parameter can be modified remotely.

There is IEEE 11073 prior art for obtaining the object containment hierarchy of a device. This information might be valuable in identification of remotely alterable parameters so long as internal object handles are not utilized.

Making it easy for frequent users

Use of the above items for security purposes is an easy enough place to start and it does provide a far more than minimal level of security for the medical device. However, it does make assumptions about what is known by the command requesting client issuing the command and what is known by the command receiving server meant to process the command. It should not be assumed than a person needing to command a device would know all of this information when making a command request from a user interface. It presumes that the application through which the person is making the request would be aware of any required identification and context information and would provide a user interface capable of easy target device selection which would implicitly provide all required identification and contextual values.

A convenient means of device selection might be to obtain the current list of devices associated with patients assigned to the requesting clinician or a list of medical devices assigned to a care unit by the CMMS system from which a clinical engineer could choose. This approach could utilize the Point of Care Identity Management Whitepaper and its follow-on profile although other approaches might be possible.

This scale of information spread across a large hospital full of command requestors (clinicians and clinical engineers) and command recipients (devices and systems) presents a large and ongoing data maintenance work effort for the hospital. The effort to load and maintain these values is beyond the scope of this white paper.

Target session confirmation by operational context

An additional level of security is possible by expecting the requestor to know and to provide in the command request the current operational session identification associated with the target medical device.

For an infusion pump or a ventilator this would be the order identifier (MDC_DMC_ATTR_ORD_ID). The clinician or Infusion Order Programmer or Infusion Order Consumer of the Point-of-care Infusion Verification Profile would be aware of this from the programming of the pump or from the patient chart.

For a physiologic monitor this might be an observation identifier (MDC_DMC_ATTR_OBS_ID), although this value is not long lasting. A monitoring order would be preferred, but those are not always communicated to the device before monitoring is started. For a spot check or vital signs monitor there is no expectation of patient specific order identification. A care unit specific blanket order identifier might be a means of providing this level of security without mandating per patient monitoring orders or per patient spot check or vital signs monitoring orders.

For an alerting device this would be identification of the alert (the alert control ID MDC_DMC_ATTR_ALRT_ID). This is the identifier for the alert and not the identifier for associated with the child update messages to the parent alert. This identifier is valid only as long as the alert is active which makes it a good target identifier for the specific alert to be affected. This is an ACM Alert Reporter to Alert Manager internally originated and communicated identifier. This would make it more difficult for systems not in that informational flow to have awareness of this identifier. While this improves security it does make it more difficult to expect clinician awareness of this identifier. An ACM Alert Consumer should also have this information, presuming it maintains a dashboard of active alerts.

17 RDC Actors and Transactions

The following figure diagrams the actors involved with this profile and the transactions between the actors.

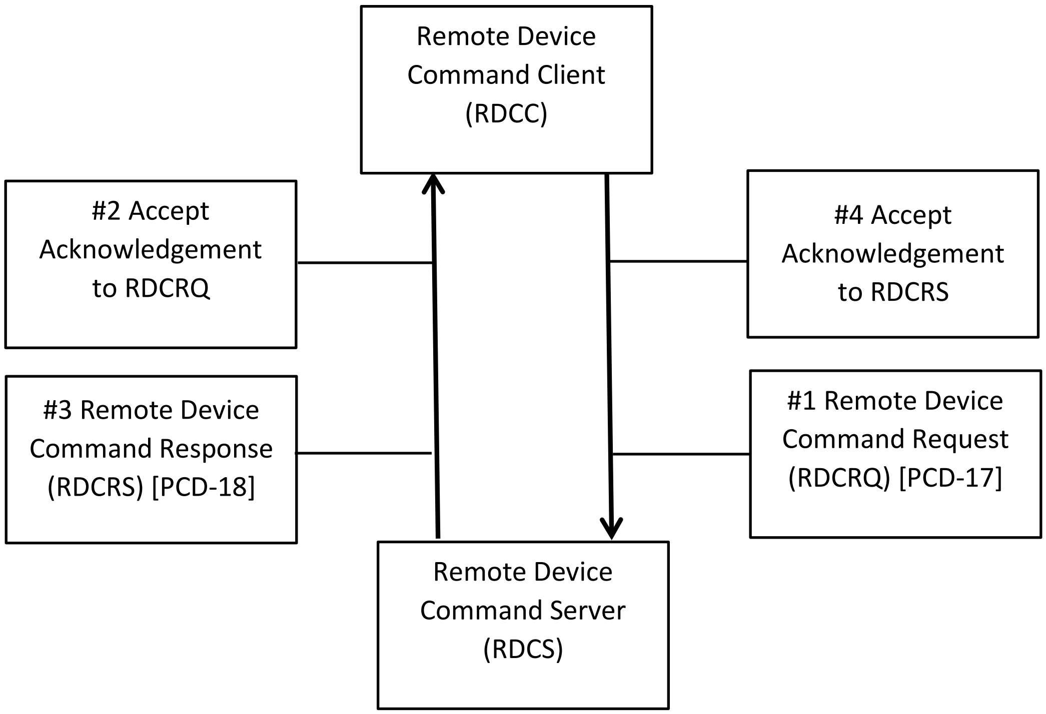

Figure 17-1: RDC Integration Profile with Actors and Transactions

Table 17-1: RDC – Actors and Transactions

Actors	Direction	Transactions	Opt.	Section in TF-2
Remote Device Command Client (RDCC)	Output	Remote Device Command Request (RDCRQ) [PCD-17]	R	Section 3.1
	Input	RDCRQ Accept Acknowledgement	R	Section 3.1
	Input	Remote Device Command Response (RDCRS) [PCD-18]	R	Section 3.1
	Output	RDCRS Accept Acknowledgement	R	Section 3.1
Remote Device Command Server (RDCS)	Input	Remote Device Command Request (RDCRQ) [PCD-17]	R	Section 3.1
	Output	RDCRQ Accept Acknowledgement	R	Section 3.1
	Output	Remote Device Command Response (RDCRS) [PCD-18]	R	Section 3.1
	Input	RDCRS Accept Acknowledgement	R	Section 3.1

Process flow

The following diagram depicts the message process flow.

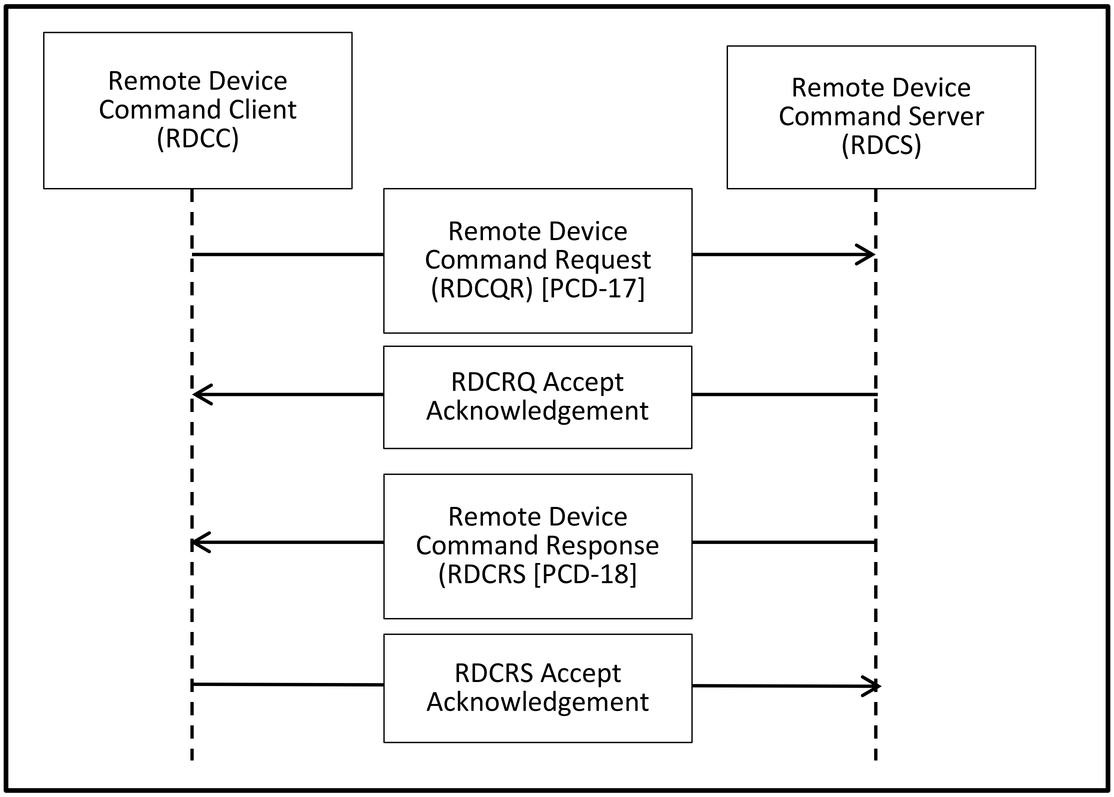

Figure 17-2: RDC Integration Profile Process Flow

18 Remote Device Command Request

As the RDCRQ message is a new transaction between new actors it would need a new PCD domain transaction identifier. PCD-17 has been chosen for interim use in this white paper. A PCD ISO OID would also need to be allocated. If this effort results in a profile supplement being produced then the transaction identifier and OID would need to be confirmed as unique and officially assigned at that time.

Protocol – HL7 version 2.6 with forward looking reference to PRT segment

Definitions and requirements – Definition and requirements indications for common HL7 message fields and components are documented in the HL7 standard, the shared PCD Technical Framework, or a specifically utilized PCD Profile are not listed here. What are listed here are the fields and components specific to device command for the use cases within scope of this document.

Segment – OBX

Awareness of the context of the object to be commanded

At least MDS, VMD, optionally CHAN.

Would need MDC/REFIDs to pass to destination (not to identify sender)

OBX-3 values

MDC_DMC_ATTR_MDS

MDC_DMC_ATTR_VMD

MDC_DMC_ATTR_CHAN

OBX-4 Values for identification of the object to be modified

OBX-5 is the value of the above items

Likely only a few forms (MDC/REFIDs) of command access identification would need to be added to 11073-10101 (a future version release, not version b)

To be carried in an OBX segment with OBX-5 as the value

Observations (from PCD-01 or PCD-10)

OBX-3 something like MDC_DMC_ATTR_OBS_ID

Specific value TBD, observation ctrl ID not long lasting

Orders (from PD-03)

OBX-3 something like MDC_DMC_ATTR_ORD_ID

Specific value likely to be the order ID

Alerts (from PCD-04)

OBX-3 something like MDC_DMC_ATTR_ALRT_ID

Specific value likely the alert control ID

OBX-2 data type should not be fixed as it is likely to be vendor actor implementation specific and so could be numeric, string, ref URL, etc.

OBX-3 would be the clue as to the meaning of the value and would be interaction use case specific.

OBX-6, OBX-7, OBX-8 would not be needed and so usage would be X.

OBX-11 would be “F”

OBX-18 or PRT-10 would be the device ID from the pertinent previous message.

The HL7 Observation segment shall be the segment used to convey the identification of a piece of equipment (a device). There can be multiple observations (OBR collections of OBX segments) per HL7 message. There can be multiple equipment identification and status reports per message, but they must be under individual OBR groupings with at most one piece of equipment per OBR grouping.

Table18-1: HL7 OBX Segment Attribute Table for Equipment Identification or Status Observation

SEQ	LEN	DT	OPT	RP/#	TBL#	ITEM#	ELEMENT NAME
2	2	ID	C		0125	00570	Value Type
3	250	CWE	R			00571	Observation Identifier
4	20	ST	RE			00572	Observation Sub-ID
5	99999	Varies	C	Y/2		00573	Observation Value
11	1	ID	R		0085	00579	Observation Result Status
14	26	TS	CE				Observation Date/Time
18	22	EI	CE	Y		01479	Equipment Instance Identifier

OBX-2 Value Type OBX-3 Observation Identifier (CWE)

This field contains the MDC code identifying the identification or status observation as for a piece of equipment.

The syntax template is

<MDC code>^<MDC string>^MDC

The field value for XXXX observation for a piece of equipment is

0^MDC_ATTR_XXXX_XXXX_XXXX^MDC

If an identifier exists for an attribute then the same identifier can be used to identify the observation as the parameter to be modified.

OBX-4 Observation Sub-ID (ST)

The content of this field is as per the PCD Technical Framework and is typically referred to as the containment hierarchy dot notation. It is used to identify the hierarchical source of an observation value within a medical device system. If the value is agreed between requestor and recipient the value of OBX-4 could be used for identification of the parameter to be modified. In the absence of such agreements and conformance to them the use of OBX-4 values for security or target identification is not recommended.

OBX-5 Observation Value

This field contains the value of the observed equipment identification or status. If this is a remote device command request then this value could be used for the requestor to supply the new value to the recipient.

Syntax Template and Value Examples

OBX-5 Value for xxxx observations.

Syntax

<xxxx>^<xxxx>^<xxxx>

Example

xxxx^xxxx^xxxx

OBX-11 Observation Result Status (ID)

The conveyed observation value is not subject to later review or correction. If the value changes it is conveyed through additional observation reports. The value of this field is therefore always indicated as "Final" using an ID of **F**.

OBX-14 Observation Date/Time (DTM)

The field contains the date and time stamp in 24-hour clock notation as of the time of the hardware or software capture of the equipment or status information for conveying as a report.

The field syntax template for the data type is

YYYY[MM[DD[HH[MM[SS[.S[S[S[S]]]]]]]]] +/-ZZZZ

A value example for 12/31/2013 at 10:15:27 PM UTC (e.g., NTP) would be

20131231221527-0000

For more information on the HL7 DTM Date/Time data format see HL7 2.6 2.A.22 DTM – date/time. The PCD Technical Framework requires time zone be indicated, and IETF RFC3339 for time zone-less (UTC) indications.

OBX-18 Equipment Instance Identifier (EI)

The value of this field identifies the equipment for which the identification or status is being reported.

Table 18-2: HL7 Sub-Component Table – EI – Entity Identifier

SEQ	LEN	DT	OPT	TBL#	SUBCOMPONENT NAME
1	199	ST	CWE		Entity Identifier
2	20	IS	CWE	0363	Namespace ID
3	199	ST	CWE		Universal ID
4	6	ID	CWE	0301	Universal ID Type

xxxx

Sub-component 1 Entity Identifier (ST)

xxxx

Sub-component 2 Namespace ID (IS)

xxxx

Sub-component 3 Universal ID (ST)

This sub-component contains a world unique value that identifies the producer of the **Namespace ID** value. In the world of PCD this would be the EUI-64 value that identifies the equipment or software vendor.

For more information on world unique identification by EUI-64 value please see the PCD Technical Framework.

Sub-component 4 Universal ID Type (ID)

This sub-component contains the type of the value in sub-component 3 **Universal ID**. At this time the use of EUI-64 cataloged values is strongly recommended by the PCD Technical Framework and so the value of this sub-component would be **EUI-64**.

The device identification can alternatively be provided in a Participate (PRT) segment child instance to the OBX segment instance.

19 Message Content for Specific Use Cases

Use Case #1 - Temporarily silencing the audio

This use case is for remote temporary silencing of an active alert.

Send Remote Device Command Request (RDCRQ PCD-17) from RDCC to RDCS

The remote command requesting client system opens a TCP socket connection to the remote command server and sends the Remote Device Command Request [PCD-17] from the RDCC to the RDCS to temporarily silence the alert.

OBR remote command

OBX type of command

OBX target device

OBX possible security information

OBX possible command parameters

In the absence of an HL7 standard message structure and type for this function the ORU_R01 message structure is utilized. It requires the inclusion of a PID segment. In this use case the patient is not known so PID-31 contains a Y. The ORU_R01 message structure requires inclusion of the PV1 segment. In this use case the ADT assigned patient location is not known so the segment is essentially empty.

Placer Order Number (OBR-2) is the command request transaction identifier as defined by the command requesting client (RDCC) actor. The Filler Order Number (OBR-3) of the request PCD-17 is empty. The identification of the context of the request is passed in an OBX segment so as not to confuse it with request and response identifiers needed for traceability of the remote device command request itself. The Universal Service Identifier (OBR-4) identifies that this is a remote device command operation request. In the OBX segment instance identified by MDC_MOC_CNTRL_OP the command target device is identified by the value in Equipment Instance Identifier (OBX-18) or through a Participate (PRT) child segment occurrence. In the OBX segments Observation Result Status (OBX-11) is indicated as final (F) as there is no clinician expected certification of the observation. The identification of the requesting individual is in either Producer's ID (OBX-15) or through a Participate (PRT) child segment occurrence.

```
MSH|^~\&|<sending application name>^vendor EUI-64 value>^EUI-
64|<sending facility>|<receiving application name>^<vendor EUI-64 value>^EUI-64|<receiving
facility>|<timestamp>||ORU^R01^ORU_R01|<control
number>|P|2.6|||AL|NE||ASCII|EN^English^ISO639||
IHE_PCD_RDC_001^IHE PCD^<OID for PCD-17>^ISO
PID||||||||||||||||||||||||||||||Y
PV1||||
OBR|1|<order number of the command request>| |528^ MDC_MOC_CNTRL_OP
|||<timestamp>

OBX|1|ST|528^MDC_MOC_CNTRL_OP|<dot
notation>|PAUSE_ALERT_AUDIO||||||F|||<timestamp>||||<identification of command
target device>||
OBX|2|CWE| [OBX MDS to identify device system]
OBX|3|CWE| [OBX VMD to identify virtual device]
[target device identified by its EUI-64 in OBX-18 or PRT-10]
[security - identify specific alert to be audio paused by its parent message number]
```

Send Accept Acknowledgement to RDCRQ (PCD-17) from RDCS to RDCC

On the same already open TCP socket connection the RDCS sends the accept acknowledgement that confirms command receipt and acceptance of request (PCD-17 ACK). Acceptance implies that any security verifications of the command request have been completed, else an ACK indicating ERR and whether or not it is a security or operational error.

On the same already open TCP socket connection receive the simple ACK that confirms command receipt and acceptance of request (PCD-17 ACK). Acceptance implies that any security verifications of the command request have been completed, else an ACK indicating ERR and whether or not it is a security or operational error.

This is the command received and requestor credentials and context verified acknowledgement from the command server back to the command originating client.

```
MSH|^~\&|<sending application vendor name>^<vendor EUI-64 number>^EUI-64|<sending
facility name>|<receiving application vendor name>^<vendor EUI-64 number>^EUI-
64|<receiving facility name>|<sending timestamp>||ACK^R01^ACK|<message control
number>|P|2.7||||||ASCII|EN^English^ISO659||IHE_PCD_RDC_001 MSA|CA|
```


Send Remote Device Command Response (RDCRS PCD-18) from RDCS to RDCC

On the same TCP socket connection receive the confirmation message from the device that the command request has been processed [PCD-18]. This will include a completion status (success/failure).

MSH ORU_R01 (for want of anything else) [PCD-17]

PID patient or not based upon the command response sender

OBR remote command

OBX type of command

OBX target device

OBX possible security information

OBX possible command parameters

On the same TCP socket connection send a simple ACK to confirm receipt of the command request completion.

Send Accept Acknowledgement to RDCRS (PCD-18) from RDCC to RDCS

Client responds with ACK

```
MSH|^~\&|<sending application vendor name>^<vendor EUI-64 number>^EUI-64|<sending facility name>|<receiving application vendor name>^<vendor EUI-64 number>^EUI-64|<receiving facility name>|<sending timestamp>||ACK^R01^ACK|<message control number>|P|2.7|||||ASCII|EN^English^ISO659||IHE_PCD_RDC_002 MSA|CA|
```

Client closes the TCP socket connection.

Use Case #2 - Clear volume infused so far

In the case of multiple infuser pumps a parameter to clearly identify the specific infuser. This may be implicit in the identification of the infusion order. Clearing of all infusers in a single command is not supported. An OBX segment occurrence identified as

```
0^ MDCX_MOC_CNTRL_OP_INFUSATE_SOURCE
```

with a value indicating a specific infuser or all would need to be a part of the command request.

Note: The request to clear infused so far shall cause pump to send an IPEC PCD-10 with an event indication of volume infused so far prior to being cleared (a new event type for IPEC). The next update produced DEC PCD-01 would reflect the volume infused following the reset.

Send Remote Device Command Request [PCD-17] from the RDCC to the RDCS

This is the request from the command originating client to the command processing server.

The remote command requesting client system opens a TCP socket connection to the remote command server and sends the remote device command [PCD-17) to reset the visual display of infused thus far.

The ORU_R01 message structure requires the inclusion of a PID segment. In this use case the patient is not known so PID-31 contains a Y.

Send Accept Acknowledgement to RDCRQ (PCD-17) from RDCS to RDCC

This is the command received and requestor credentials and context verified acknowledgement from the command server back to the command originating client.

```
MSH|^~\&|<sending application vendor name>^<vendor EUI-64 number>^EUI-64|<sending
facility name>|<receiving application vendor name>^<vendor EUI-64 number>^EUI-
64|<receiving facility name>|<sending timestamp>||ACK^R01^ACK|<message control
number>|P|2.7|||||ASCII|EN^English^ISO659||IHE_PCD_RDC_001 MSA|CA|
```

Send Remote Device Command Response (RDCRS PCD-18) from RDCS to RDCC

Send Accept Acknowledgement to RDCRS (PCD-18) from RDCC to RDCS

```
MSH|^~\&|<sending application vendor name>^<vendor EUI-64 number>^EUI-64|<sending
facility name>|<receiving application vendor name>^<vendor EUI-64 number>^EUI-
64|<receiving facility name>|<sending timestamp>||ACK^R01^ACK|<message control
number>|P|2.7|||||ASCII|EN^English^ISO659||IHE_PCD_RDC_002 MSA|CA|
```

Use Case #3 – Remote unlock of device operator panel

Send Remote Device Command Request (RDCRQ PCD-17) from the RDCC to the (RDCS

This is the request from the command originating client to the command processing server.

The remote command requesting client system opens a TCP socket connection to the remote command server and sends the remote device command (PD-17) including the unlock level and unlock code to unlock the device operator panel.

Send Accept Acknowledgement to RDCRQ (PCD-17) from RDCS to RDCC

This is the command received and requestor credentials and context verified acknowledgement from the command server back to the command originating client.

```
MSH|^~\&|<sending application vendor name>^<vendor EUI-64 number>^EUI-64|<sending
facility name>|<receiving application vendor name>^<vendor EUI-64 number>^EUI-
64|<receiving facility  name>|<sending timestamp>||ACK^R01^ACK|<message control
number>|P|2.7|||||ASCII|EN^English^ISO659||IHE_PCD_RDC_001 MSA|CA|
```

Send Remote Device Command Response (RDCRS PCD-18) from RDCS to RDCC

Send Accept Acknowledgement to RDCRS (PCD-18) from RDCC to RDCS

MSH|^~\&|<sending application vendor name>^<vendor EUI-64 number>^EUI-64|<sending facility name>|<receiving application vendor name>^<vendor EUI-64 number>^EUI-64|<receiving facility name>|<sending timestamp>||ACK^R01^ACK|<message control number>|P|2.7||||||ASCII|EN^English^ISO659||IHE_PCD_RDC_002 MSA|CA|

20 Futures

In the future, it might be possible to add standards data for NIST verification (RTMMS, MDC/11073, HL7, etc.).