Integrating the Healthcare Enterprise

IHE Patient Care Device (PCD) White Paper

Point-of-Care Identity Management (PCIM)

Published

Revision 1.1

Date: June 16, 2017

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 June 16, 2017. 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

1 Purpose

In modern acute-care medicine, electronically sensed observations of a patient's physiological state make a key contribution in the clinical treatment of acutely ill patients. Medical devices that act on a patient, such as devices controlling the delivery of a drug infusion, also send and receive data and commands electronically. Clinicians must be able to rely on the accuracy, currency, completeness and routing of the electronic messages between these devices and systems; otherwise the data or the therapy may be harmful rather than helpful. This is similar to the "five rights" of medication administration ("the right patient, the right drug, the right dose, the right route, and the right time"), but here it is "right patient, right devices, right time". Every measurement must go to the right chart, every chart must have every measurement, and every device command affecting a patient must reliably be sent to the correct device acting on that patient.

A correct electronic record of a patient's medical state depends on correct knowledge of what medical devices are observing and acting on that patient in the present, and at past times in the patient record. We will call the connection between a patient and each relevant medical device, the device-patient association. A device-patient association has a beginning and an end, and incorrect or untimely recording of these events can lead to harmful results.

The purpose of this document is:

- to review use cases and system architectures in which electronic information exchanges about device-patient associations may and may not be beneficial
- discuss risk analysis approaches that may be appropriate for institutions reviewing their risks of data misdirection due to incomplete, incorrect, or untimely device-patient association assumptions
- suggest basic electronic messaging formats for reporting, collecting, disseminating and querying device-patient associations

1.1 Intended Audience

The intended audience of the IHE PCD Point of Care Identity Management White Paper is:

- Clinicians involved in the collection and use of real-time clinical data in acute care environments, and others interested in integrating healthcare information systems and workflows in acute care environments.
- Experts involved in risk analysis and profile development, from healthcare institutions, device and system manufacturers, and regulatory agencies.

1.2 Comment Process

Comments are particularly desired from clinicians and other healthcare professionals concerning additional requirements that should be considered, potential additional sources of errors, and ways to improve workflows contemplated in the analysis.

Additionally, comments are desired from technical experts from healthcare institutions, manufacturers and other interested parties concerning ways the proposed means for identity management can be improved.

IHE International welcomes comments on this document and the IHE initiative. Comments on the IHE initiative can be submitted by sending an email to the co-chairs and secretary of the Patient Care Device domain committees at pcd@ihe.net. Comments on this document can be submitted at http://www.ihe.net/PCD_Public_Comments.

1.3 Acknowledgements

The members of the Work Group, present and past, who have contributed to this document are gratefully acknowledged, as well as others who have contributed comments (and with apologies to anyone overlooked in this list). This includes (in alphabetical order): Chris Courville (Epic), Al Engelbert (Protolink), Robert Flanders (GE), Gary Meyer (BD), Kosta Makrodimitris (FDA), Doug Pratt (Cerner), John Rhoads (Philips, work group lead), Stan Wiley (Draeger). Special thanks to Ioana Singureanu, whose early analysis of this problem in HL7®[1] Detailed Clinical Models for Medical Devices (Singureanu 2015) is important and is partly reproduced in Appendix B, though she does not necessarily agree with the propositions in this white paper.

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

2 Problem Description

This white paper considers current practices for tracking device-patient associations; that is, assuring that the data flows from communicating patient care devices are associated with the right patient in a timely and reliable way. It asks the question of how facilitating communications among the electronic systems involved can make such associations both more consistent and reliable for clinicians to manage in particular use cases while not needlessly impeding workflow. It will present the general technical features of an implementable approach for information exchanges to support flexible implementation of more reliable procedures. These information exchanges are intended to serve as the basis for a new profile in the IHE Patient Care Device Domain.

Although compared with connectivity and semantic interoperability in getting data from devices into electronic medical records and other hospital computer systems, the pitfalls in logically associating devices with patients in real time have received relatively little attention in standards. But the safety risks of incorrect device-patient association have been highlighted many times (ECRI Institute 2013b; ECRI Institute Patient Safety Organization 2012; ECRI Institute 2013a, 2015; Melendez 2012, 2014; Zaleski 2015).

Possible errors include:

- Failing to record the association as having been established at the point in time when it occurred, leading to an incomplete record. Possible mitigations include technical support enabling a simple workflow step at the point-of-care to electronically record the event of starting data flow for a set of devices.
- Failing to record that the association had been terminated at the point in time when the device was disconnected from the patient, leading potentially to the spurious addition of data from another patient to the record. Usually device-patient disassociation, that is, the end of device data collection for a patient from devices, is a less salient event in care workflow than setting up the patient and starting the device data flow, so special mitigations in the workflow may be indicated to ensure that incorrect device-patient associations are not wrongly left in place. An example would adding a device-patient association check to a checklist executed when the patient is to be moved. Automated mitigation measures could include, for example, the device-patient association manager using algorithms checking message timestamps to determine that a device is associated with a patient and yet hasn't originated data for long time, or that there are probable conflicting assignments in effect (associations of a patient with monitors at two different fixed locations, for instance).
- Creating an association of data flows from a device or to a device with the wrong patient. Mitigated by confirmation by an authorized person at the point of care able to visually check all device-patient associations.

Any of these, if not recognized, can lead to treating a patient on the basis of incomplete or incorrect data, with potentially serious harm to the patient.

Establishing correctly and completely the relationship between the flows of data from (and to) the patient care devices at a point of care, and the identity of the patient actually being observed

and treated, is critical to creating a correct and complete real-time display and retrospective patient record. It is a collaboration between the clinicians at the point of care, the devices and supporting electronic systems there, and the systems that are receiving, curating, and using the data, principally electronic medical records systems and clinical decision support systems.

Device and device gateway systems provide facilities for associating devices with patients and sending the resulting patient identity information in their data feeds to other hospital systems such as EMRs. An indication that many health care delivery organizations (HDOs) do not have confidence in the patient identity information provided in this way is that their systems disregard this information in the data feed and base all their device-patient data linking on other sources (Luis Melendez, Partners Healthcare, personal communication 2013).

It may be that an HDO has already determined that its workflow processes reduce the risk of errors in its medical records due to faults in device-patient association to an acceptable level. For organizations that have not yet applied systematic risk analysis to the issue, though, this document presents suggestions about methods for carrying out such an analysis, some of the hazards to be considered, and possible mitigations to be considered for further reduction of risk. Some possible mitigations are technical, and involve information exchanges. It is a further intention of this paper to suggest transactional information exchanges for a possible, future IHE Patient Care Device Integration Profile to support accurate recording of the device context of the patient, the patient context of the device, and to promote flexible integration of information for "situational awareness" by the devices, systems, and personnel.

The proposed transactions do not restrict the possible architectural relations among systems involved in tracking the patient identities, the device identities, and the device-patient associations. Actual implementation choices would depend on the capabilities and site-specific use cases, and analysis of the level of risk of a particular HDO. It is assumed that responsibility for patient identity management will stay with existing admit / discharge / transfer and/or master patient index systems and will rely on IHE ITI demographic and patient encounter transactions. The interface for confirming device-patient associations at the point of care could be supported by a mobile device or an additional user interface screen of an EMR, a device or a device gateway. The database functions of maintaining a list of candidate devices for association could involve a collaboration with a computerized maintenance system or other systems maintaining a database of at least some devices, such as a monitoring network management application. Maintaining a database of the specific associations of devices with patients could be a modular capability added to an existing system (such as EMR, device management software or general hospital database system) rather than necessarily a new standalone system.

2.1 Initial Problem Definition

The IHE PCD Point-of Care Identity Management (PCIM) Work Group has been created to analyze the practical problems of associating automatically-collected medical device data reliably with patient identity to promote accuracy and completeness of medical device data in electronic medical records (EMR). We identified use cases where no additional information exchange transactions appeared to be needed, but we also noted cases for which we could find no existing profile which met the need for information exchange that have been requested by systems designers. These requests have included:

- A means for listing candidate devices to be displayed to a clinician at the point of care (for example, on a handheld device or smart phone) so that the right ones may be associated with a patient, to allow for establishing confirmed associations by a qualified person who is able to see the actual situation in real time.
- Explicit notification of, for example, an EMR system by a device or device gateway, or a specialized system for maintaining device-patient associations, of what devices are associated with the patient on the basis of confirmed observations at the point of care.
- A facility for a device, gateway system or other system to query a system maintaining a database of associations for a list of current and past device associations for a patient, or patient associations for a device, also providing for a "publish-subscribe" mechanism for the querying system to obtain ongoing updates on device-patient association and disassociation events.

This white paper introduces new IHE transactions for study and possible prototyping. These newly proposed transactions are intended to improve device-patient identity binding as a step towards the desired state of reducing the risk of the incorrect device data in the electronic medical record of a patient.

In this paper we will use the term 'patient identity management' to refer to all of the processes involved in maintaining consistent patient identity information, including but not limited to:

- identity proofing (in particular, determining a unique, invariant patient identifier in the registration process)
- workflow procedures such as scanning patient wristbands to support assuring that the patient's identity is always correctly known throughout all episodes of care in the institution
- seeing that the patient identifier and sufficient other identity factors such as name and date of birth are consistently included in all electronic records
- the process of linking electronic patient information between different episodes of care in an institution, and linking medical records of the patient from other institutions

Patient identity management is a precondition for device-patient association, and there must be similar processes for managing identities of devices.

In the 2009 HIMSS white paper on Patient Identity Integrity (HIMSS Patient Identity Integrity Work Group 2009), the holistic process for matching records for one individual person across and within multiple EMRs, potentially held by different institutions, was presented systematically. The main focus of that study was the problem that is key in Health Information Exchanges, the matching of health records containing information on the same patient by matching identifiers accompanying the records. Two key problems were identified among others: device incompatibility (data incompatibility due to no common format means or lack of data interoperability for exchanging data) and the quality of data that is used for patient-record matching.

Device compatibility has been addressed through subsequent releases of communication profiles such as the IHE Patient Care Device domain's Device Enterprise Communications Profile and others. Improving the quality of data at the point of care was still recognized as an unmet need, particularly in government agencies. A report with suggestions for government agencies concerned with patient identity (NorthPage Research 2010) strongly identified proposed automation of patient identity management integration and delivery as one of 5 tips for successful patient identity management in Government Agencies.

2.1.1 How Point-of-Care Identity management differs from other patient identity problems

2.1.1.1 Cross-institution health information exchanges.

Most of the literature concerned with patient identity management deals with multiple electronic medical records existing in different systems, often in different institutions, and the question of whether records which appear to pertain to the same patient actually do, and whether therefore the records can be safely joined to give a fuller picture of the patient's health history. Such a joining would need to be supported by evidence leading to an assessment of the likelihood of the records applying to the same patient based on identity attributes that can be compared between the records. The attributes, such as name, age or date of birth and so on, taken singly, do not in general identify an individual uniquely and, further, are subject to recording and other errors. So the challenge in that situation is assessing the combined value of the identifying attributes that are common between the records, and determining whether the combined evidence is sufficient to support joining the records to allow clinicians access to fuller information on the patient.

An environmental scan performed by ONC (Office of the National Coordinator for Health Information Technology 2014) recognized that "the lack of data attributes that are populated consistently and in a standardized format within messages…[is] a major impediment to more accurate patient matching." Many other publications in the large literature on patient matching touch tangentially on the problems of improper matching of patient identity with device data.

2.1.1.2 In-hospital association of device data flows with patients.

The problem treated in the present paper is distinct from this general record linkage problem. It arises from the way that, in the course of their care while admitted to a hospital, patients can be expected to have different monitoring and therapy devices that are able to report observations electronically, connected to them at different times as their care needs change and as they may move from location to location within the healthcare provider institution. This paper concerns the means, procedures, and processes by which the records of therapy and monitoring are at all times going to the correct patient record, and also that data will not be missing from the patient record unnecessarily because of incomplete or missing identifying information.

Here in this whitepaper, the situation is that the patient is being treated and observations are being automatically collected and recorded at a healthcare provider institution, and the patient is assumed to have been registered in the institution's admission system and assigned a known, unique institutional identity number. An exception to this assumption that is still within the scope of this study: when a patient is being treated on such an urgent basis that the identification and

registration process is not completed until after treatment has begun and observations have been recorded. But in this case, it is assumed that identification and registration will be done when feasible, and once it is done, that the observations recorded prior to the full identification of the patient will then be linked to the patient record, so that they may later be reviewed together with other data about the patient.

2.2 Desired State

The goal of this white paper is to assist in improving reliability, and hence safety, of association of device data with patients by suggesting risk analysis considerations for workflows and system design, and give preliminary specifications of electronic information exchanges based on profiling HL7 messages to allow systems to exchange information verified by clinicians at the point-of-care. There have been publications, for example Frisch et al. (2009) and proprietary systems featuring ideas very similar to what is proposed in this white paper. The purpose of this paper is to start the development of standards-based communications exchanges to support vendor-independent implementations of these ideas.

2.2.1 Reasons for creating a new profile in Patient Care Device Technical Framework

Current IHE PCD Profiles, specifically Device Enterprise Communications, deal with standardized observation reporting for device data and specify how patient identifying information shall be sent with device observations. The scope of these profiles does not cover some use cases for how the patient identifying information is obtained and verified. The present work is to discuss additional use cases, and means for recording events of devices becoming associated with patients, and means for systems to receive notifications of such events, as well as to query the state of associations.

2.2.2 Reasons for selecting HL7 v2.6 with use of PRT segment drawn from v2.7 and Unique Device Identifier from v2.8.2

Profiles in the IHE Patient Care Device domain currently use a base HL7 version of 2.6. However, it has been the practice of IHE PCD to include material from more recent versions of HL7 when they provide important new capabilities of value in a particular profile. So in this profile, we use the PRT Participation segment first defined in HL7 Version 2.7, and we also use the extensions to the PRT segment to accommodate the Unique Device Identification data items defined by the US FDA included in HL7 Version 2.8.2. (In 2013, the Food and Drug Administration (FDA) released a final rule establishing a Unique Device Identification system designed to adequately identify devices through distribution and use which requires device labelers to include a unique device identifier (UDI) on device labels and packages so this is provided for in this profile).

2.2.3 Other HL7 approaches that were considered but not chosen

Other approaches considered but not selected included Scheduling messages as in HL7 Ch.10. While there is some logical relationship between scheduling equipment to be used on a patient and identifying the equipment that is communicating clinical data, the workflows envisioned in

the design of the scheduling messages do not fit the current problem very closely. Because there is a closer relationship between the events considered here and HL7 observation reporting, we chose to base the messages on an extension of observation reporting.

2.3 General device use models

Melendez (2014) divides the interoperating medical devices of concern in this paper into fixed, mobile, and transient.

2.3.1 Fixed (location-based) device association

When a device is typically used in a specific care location, this fact is often used as a central cohesive element in device-patient association in electronic systems. An example might be a bedside patient monitor or a ventilator that is ordinarily not moved from a particular ICU bed, operating room or procedure room. In this case, the location information from the ADT system would be useful in associating a patient recorded in that bed with the fixed devices, though since this ADT information is not necessarily generated at the point-of-care and synchronous with the real situation there, it would need to be confirmed at the point-of-care. Many device systems or device gateway systems are capable of taking information in HL7 form from an ADT system and presenting it for confirmation by an operator at the device, or alternatively giving a "pick list" of candidate patients to be associated with the device. Then the device is able to integrate the patient identity data into its observation recording messages.

This essence of these cases have been well-described and analyzed by Ioana Singureanu and colleagues in the HL7 Detailed Clinical Models for Medical Devices (Singureanu 2015). See appendix B for discussion and interaction diagrams from that publication.

This method is comprehensive if the device or gateway system covers *all* the devices connected to the patient. This can be the case if additional devices that aren't generally used at a fixed bed or procedure are interfaced through, say, the patient monitor or the device gateway system that is able to mark the data as to what patient they are associated with. But if coverage is not complete, as for example for devices that are frequently moved (such as infusion pumps) the associations for these devices must be separately maintained, and there is a potential source for error. Or, in the case of infusion pumps, their data flows through a proprietary controller system that is separate from the system that is consolidating the other patient data.

2.3.2 Mobile device association

As has just been noted, the location of the patient is not always a strong indicator of the particular devices with which the patient may be associated. Ventilators, infusion pumps and other systems may be frequently moved from location to location, being associated with different patients at different times. There are also times when patient data is temporarily coming from transport monitors or transport ventilators while the patient is being moved, or from telemetry packs while the patient is ambulatory. Mobile devices outside the hospital also must be associated with a patient. These use cases create transitions in device-patient associations which must be provided for in a system design.

2.3.3 Transient, dynamic (spot-check) device association

435 Another important use case arises for devices that are to be associated with an episodic "spot-check" measurement, and then the device is moved onto the next patient. Here the device-patient association is highly transitory, but it is just as important to have a verified association to the patient.

3 Safety considerations

3.1 Unlinked data

Unlinked data are not linked to any registered patient, perhaps through emergency admission of an unregistered patient to a unit, and connection of devices to that patient with the not-yet-fulfilled intent to identify that patient to the systems concerned when the preconditions are met (registered identity available and an authorized person is available to confirm the association to the electronic systems).

This type of error is hazardous since later treatment can be based on an incomplete view of the observations that have been made on the patient if the data taken before the identity of the patient is confirmed is not joined with data taken after the identity is confirmed.

Unlinked data can also be created if an additional device is connected with the patient but the change in the set of devices associated with the patient is not noted and confirmed.

The system data flow and workflow must provide for properly associating this data after the fact, usually through creating the needed links in the EMR program. Records of device-patient association events could be helpful in confidently and reliability carrying out these operations.

3.2 Wrongly linked data

Wrongly linked data are data linked to the wrong patient, either through incorrectly trusting erroneous data from another system, error in associating data with the right patient and the right device at the point of care, or failure to change the association of the device when the patient changes.

This type of error is hazardous since treatment can be based on a wrong appraisal of the state of the patient.

One implication of this is that the information of when a device-patient association is broken by taking the patient off the device is quite as critical as when the device-patient association begins. Weaknesses in workflow procedures that could lead to missed transitions between patients connected to devices should be looked for in risk analyses.

4 Risk Analysis

A healthcare delivery organization that is considering changes to their procedures for associating patients with data from devices should perform a systematic risk analysis using current best practices for such analyses where medical devices are involved (IEC 2009; ISO 2007), also surveying other relevant standards recognized by the appropriate regulatory entities: in the U.S., for example, standards listed by the U.S. Food and Drug Administration (2015), and the frequently updated online database of recognized standards. Even if no particular change in procedures or systems is being considered, if no risk analysis of existing workflows and procedures for device-patient association has been done previously, it can be beneficial to go through the process of preparing one.

Although the focus is somewhat different, the "IEC 80001-1, Application of risk management for IT-networks incorporating medical device—Part 1: Roles, responsibilities and activities" (IEC 2010) and other standards and reports in this series contain a great deal of valuable information about how an organization can prepare for, execute, and maintain risk analyses with participation by clinical and technical management, and the responsibilities of software and equipment vendors to provide adequate information on their products to enable such analyses.

Because HDOs, and indeed units within HDOs, differ in their equipment, workflows and rules it is not possible to make a universally applicable "one-size-fits-all" analysis of risk so this white paper will limit itself to suggesting some widely relevant hazards and causes that such an analysis should take into account, together with other hazards that may be identified by the team in their particular environment.

Incorrect association of device data with patients has been identified as a safety risk (ECRI 2015). The probability of adverse effects depends on the detailed circumstances in a particular care environment and should be part of an integrated risk analysis.

Workflows may use information from admit, discharge, transfer systems in associating patients with particular point-of-care locations and therefore particular fixed equipment (for example bedside patient monitors). This information can be valuable in establishing device-patient associations, but the ADT events and messages are not necessarily synchronized with the actual presence of the patient at the location and the actual connection of the equipment to the patient. Additionally, in the case of the patient monitor, although it may act as an intermediary and a data source for transmitting data originating in other devices, it is not necessarily a source for all the important device data concerning the patient: there may be other devices not connected to it, such as infusion pumps or a ventilator. These must be separately accounted for.

Consequently, it is important for a workflow to include provision for an authorized clinician in the patient vicinity, aware of the patient's situation and able to see the devices, to verify the accuracy and completeness of the list of devices originating data about the patient. Because this is an important safety precaution and because clinicians are frequently overburdened, part of the intention of this white paper is to suggest ways that this verification step can be made easily and without needless waste of time by providing for the centralization of this information in a single user interface. This interface could be provided at an EMR viewing station, or at a device such as a monitor or data gateway system, or on a mobile device with wireless access to patient and device identity information.

Hazard	Causes and contributing factors	Mitigations considered
Treatment delayed or incorrect	With monitoring device, relying on ADT admit message when message is delayed until after patient has been connected with device, and observation has begun	
	With therapy device, relying on ADT admit message when message is delayed until after patient has been connected with device and observations or treatment has begun	
	Relying on ADT admit when message is received prior to patient's actual presence in the unit, connected with the "expected" devices.	

4.1 Requirements for associating device data with patients

Recording of data to the patient's record must reflect the exact start of when correct data are able to be reported from a particular device.

Recording of data to the patient's record must reflect the exact time when that patient is no longer connected to that device. It may not be technically feasible to do this on a completely automatic basis. For example, the disconnection of leads or transducers from a patient may be easy to detect, but knowing whether this is unintended by the caregivers, or whether it may be intended but meant to be temporary (e.g., when data must be interrupted for a particular care procedure, with the intention that the data will be resumed as soon as possible). Then when data collection is resumed, the device generally has no way of determining if the data is actually coming from a different patient without being given that information by a clinician.

So, as a concomitant of starting or stopping the use of a monitoring or therapy device, there must be:

1. A means of providing, and when possible, eliciting, confirmation by an authorized person of what patient the device is associated with, based on multiple identity factors where appropriate.
2. A means of communicating such a confirmation to the system of systems supporting the creation of an electronic medical record, with its supporting details such as the patient identifier read from the patient's bar code, the unique identifying code of the device connected to the patient, and the authorized person confirming the association.
3. A means of assuring that caregivers are cued when a patient has been disconnected from a device, or in the worst case cuing caregivers when connecting a new patient. This could involve noting when a device is in standby state or idle for a prolonged period. It is necessary to differentiate when the absence of connection to a patient is an expected episode in care and expected to return (e.g., patient is in radiology, in transport or ambulatory and connected to a different device), or the patient is no longer at the particular point of care and not expected to return. Note also that the same measurement for a patient may come from different devices at different times, for example from a bedside monitor at some times, but from a transport monitor or a telemetry unit at other times.

4. A means for systems needing the information to have a query about the state and history of the association between the patient and all related devices (where the system making the query may be the device itself).
5. A suggested process for an institution to analyze the risks associated with their technical processes and personnel procedures and workflows for assuring correct device-patient association records.

4.2 Device-Patient Association Workflows

Any workflow involving automatically collected data will have a provision for validation of data by a clinician. If clinician validation is via a flowsheet, then device observation data must be available in the flow sheet to be validated, but it may not be included if the device-patient association was missed.

One way of establishing logical device-patient association would be to make a record at the time a device is physically connected to the patient. This could reduce the risk of missing or improperly associated data. Creation of such a real-time record could be supported by a user interface at the point of care, on a device or on a point-of-care computer system allowing for some combination of identifying means for the patient, the devices, and the authorized person initiating the record.

One aid to accurate recording would be the scanning of barcodes identifying the device or devices being connected to the patient, and the authorized person confirming the act of association.

Barcodes are not the only possible way of conveying this information. Example alternatives include the presentation of a pick-list of candidate entities (devices, patients, caregivers) and RFID devices providing a similar list of candidate entities. An essential part of this process, though, is human confirmation that the device-patient associations about to be asserted have been visually confirmed.

5 Introduction to Proposed Transactions

This implementation relies on existing IHE ITI profiles, specifically Patient Administration Management (PAM, ITI-30) and Patient Encounter Management (PEM, ITI-31) Profiles for subscribing to ADT (admit, discharge, transfer) messages to maintain a record of patient identities to be offered as candidate identities in patient pick lists, or to fill in additional demographic information needed by Device Observation Reporters in IHE PCD Device Enterprise Communications (DEC) or Alert Communications Management (ACM).

These identity and demographic information could alternatively be served by IHE ITI Patient Demographic Query (PDQ) Profile, and this might be better from the point of view of appropriate separation of concerns since use of PAM and PEM Profiles to maintain a local database of patient identity at the point of care goes against the concept of a "single source of truth" for patient identity data.

Depending on implementation details of the device-patient association maintenance, other IHE ITI profiles would be vital, particularly Enterprise User Authentication (EUA) and Patient Synchronized Applications (PSA).

At various stages of the development of this white paper, it was suggested that device-patient association might better be treated by IHE ITI as an extension of Patient Administration Management. This is a possibility, but the consensus was that device-patient association was a sufficiently different concern, and had sufficient device-specific content, that it was appropriate to develop as an IHE PCD effort.

The proposed PCIM Profile does not require a particular architecture or topology for data flows about device-patient associations; instead, it provides transactions for any appropriate system to originate assertions about such associations, and it also provides transactions for any appropriate system to query for the existence or history of such associations.

The proposed PCIM Profile has as part of its goal supporting a single authoritative source for device-patient associations, that is, a system (the Device-Patient Association Manager) that records messages from other systems (Device-Patient Association Reporters), such as an operator interface that allows selection of valid known unique patient identities, and valid known unique identities of devices (registered by a Device Registrant), or an operator interface on the device itself allowing the selection of unique patient identifiers.

Equally important is an operator interface that allows the termination of a device-patient association.

The Device-Patient Association Manager can be queried by systems needing to know the state of device-patient associations (Device-Patient Association Consumer).

5.1 Actors

5.1.1 Device-Patient Association Reporter

A system or person that asserts a device-patient association, disassociation, or attributes related to either.

5.1.2 Device-Patient Association Manager

A system that records, manages, and serves records of device-patient associations.

5.1.3 Device-Patient Association Consumer

A system or person that queries a Device-Patient Association Manager for device-patient association records.

5.1.4 Device Registrant

A system (including the device itself) or person that identifies a device that may participate in device-patient associations.

5.1.5 Patient Registration System

A system that identifies patients that may participate in device-patient associations, typically a master patient index (MPI) or other ADT system.

5.2 Transaction Use Cases

5.2.1 Device-Patient Association Reporter to Device-Patient Association Manager

- An Association Reporter asserts a device-patient association to an Association Manager.
- An Association Reporter asserts a device-patient disassociation to an Association Manager.
- An Association Reporter updates device-patient association information to an Association Manager.
- The aforementioned association/disassociation information shall include the following attributes:
- Status (asserted, confirmed, erroneous, etc.)
- Method (location, scanned device and wristband, etc.)
- Time parameters (effective begin and end times, related event times)
- Performing participant
- Patient Identifier(s)

5.2.2 Device-Patient Association Consumer to Device-Patient Association Manager

An Association Consumer queries an Association Manager, providing some combination of the following parameters:

- Patient Identifier(s)
- Device Identifier(s)

- Time Range
- Additional Filters

The Device-Patient Association Manager responds with a list of associations that satisfy the query parameters.

5.2.3 Device Registrant to Device-Patient Association Manager

A Device Registrant registers a device with the Association Manager. It may provide:

- Device identifier(s) – required.
- Device location.
- Network address if device is directly connected to the network. Omit if device data is sourced through a device gateway system.
- Communications attributes.
- Device attributes (type, make, model, etc.).
- Device features.
- Status and availability.

A Device Registrant notifies the Association Manager of updated device attributes from the list above.

5.2.4 A Device Registrant de-registers a device with the Association Manager

This transaction is for future definition and is not further detailed in this document.

5.2.5 Patient Registration System to Device-Patient Association Manager

A Patient Registration System notifies the Association Manager of a patient that may participate in a Device-Patient association. It may provide:

- Patient identifier(s) – required
- Patient name
- Patient location
- Additional attributes found on HL7 ADT messages

A Patient Registration System notifies the Association Manager of updated patient attributes from the list above.

A Patient Registration System notifies the Device-Patient Association Manager that a patient is no longer able to participate in a device-patient association.

5.2.6 Device Observation Reporter to Device Observation Consumer

A Device Observation Reporter plays the role of a Device-Patient Association Consumer to retrieve the identity of the patient to whom the observation belongs.

Once Device-Patient associations are known by the Device Observation Reporter, that system can now include this information in the observation message that it sends to the Device Observation Consumer.

This is covered in the DEC Profile (IHE PCD-01), and is listed here only to show an example of a beneficiary of this profile. Specifically, this profile enables devices to report observations with patient identification.

5.3 Effects on the system

5.3.1 Prerequisites for Association Reporter / Device-Patient Association Manager / Device-Patient Association Consumer:

In order for any actor described above to confidently report, manage, or consume the assertion of device-patient associations, the following pre-requisite conditions must be met:

1. The system must maintain an up to date database of patient records (including all of the demographic data points relevant to the device-patient association) as reported by the Patient Registration System.
2. The system must maintain an up to date database of discrete device identifiers that could be associated to a patient as reported by Device Registrant(s).
3. Future Addition: Processes should be established for actors to self-evaluate the status and integrity of both their patient record and device record databases, with said status potentially impacting the strength of the binding as reported, managed, or consumed by said actor.

5.3.2 Effects on Association Reporter:

Reporting Association/Disassociation - The action of asserting a device-patient association or disassociation by the Association Reporter to the Association Manager should include:

- Establishing a record of association/disassociation assertion between patient and device within the Device-Patient Association Reporter system, including start time, end time and association information.
- Triggering messaging to the Device-Patient Association Manager system asserting association/disassociation between patient and device, including start time, end time and association information.
- Receiving Acknowledgement - The Association Reporter should expect to receive application acknowledgement from the Device-Patient Association Manager detailing acceptance or rejection of the device-patient association.
    - On receipt of acceptance acknowledgement, the Association Reporter should internally document this acceptance (including timestamp) in a way that is linked to the original recorded instance of association.
    - On receipt of rejection acknowledgement, the Association Reporter should internally document this rejection, and present said rejection to a user or process for resolution.

5.3.3 Effects of Association and Disassociation Messages on Device-Patient Association Manager:

Receiving Association Assertion – Upon receiving a device-patient association or disassociation message from the Association Reporter the Association Manager should:

- Evaluate the validity of the assertion based on knowledge of current patient status as received from the Patient Registration System and current device status as received from the Device Registrant. Resolve any detected conflicts with confirmation by an authorized user able to check the actual situation.
- Respond to the Association Reporter with application acknowledgement detailing acceptance or rejection of the assertion.
- Establish a record of received assertions, including acceptance or rejection of the assertion, start and end times, and all related association information.

Receiving Association Query – Upon receiving a device-patient association query from an Association Consumer the Association Manager should:

- Evaluate the validity of the received query parameters based on knowledge of current patient status as received from the Patient Registration System.
- Respond to the Device-Patient Association Consumer with documented associations that fit the received query parameters, or with details regarding rejection of received query parameters when applicable.
- Establish a record of received queries, including acceptance or rejection of the query parameters, start and end times, and all related association information.

5.3.4 Effects of Association and Disassociation Messages on Device-Patient Association Consumer:

Sending Association Query – The action of querying an Association Manager for device-patient associations should include:

Triggering messaging to the Device-Patient Association Manager system with query parameters, which can include Patient Identifier(s), Device Identifier(s), time range, and additional filters.

Establish a record of sent queries, including related query parameters.

Receiving Association Query Response – Upon receiving a device-patient association query response from an Association Manager the Association Consumer should:

- Internally document the received associations and present these associations to a user or process as appropriate for future use with associated device observations.
- Check with its stored state information, and seek to resolve conflicting information, with confirmation by an authorized user if appropriate.

On receipt of query rejection response, the Association Consumer should internally document the rejection, and present said rejection to a user or process for resolution.

5.3.5 Overall Effects – Operational Considerations

Device Association Manager: Establishing a Device Association Manager "source-of-truth" system and its associated user interface allows care providers to identify instances of device-patient association and disassociation and manage the assertion or revision of these associations.

Device Association Reporter: This proposed implementation allows for flexibility in the source of the device-patient association assertion, as any assertion made by the reporter is then evaluated and tracked by the Device Association Manager and once confirmed can be accessed by other reporters and consumers in the organization.

Device Association Consumer: This proposed implementation also allows for flexibility on the consumer of device-patient associations, as responsibility for the assertion can be entirely moved to manager and reporter actors or the assertions received by the consumer can be additionally validated through a user interface associated with the consumer.

5.3.6 Overall Effects – Organizational Considerations

Anticipated improvements include:

- Single authoritative reference system or "source-of-truth": Establishing a Device Association Manager in an organization introduces a central point where all covered device-patient associations can be viewed, evaluated, and revised. This also allows for robust reporting and root-cause analysis for any adverse events that occur where incorrect device-patient associations play a role.
- Flexibility in association methods: The flexibility of actor topology as described in the proposed implementation allows the organization to design workflows for device-patient association specific to its needs and patient-care contexts, and allows for such association workflows to be enhanced and updated as viewed necessary.
- Human participation in assertion: The workflows supported in the proposed implementation include points of assertion acceptance or rejection, requiring evaluation of the assertion rather than automatic acceptance. The intention is to allow not only for technology-based verification but also involvement and validation by participating care providers, providing additional layers of safety.

5.3.7 Overall Effects – Implementation Considerations

In addition to the anticipated improvements to the organization as described above, the following are deployment impacts that should be considered:

- Requirement of Device Association Manager System: The proposed implementation requires the existence and implementation of a Device Association Manager system. Such a system is likely not in place in the existing topology of the organization, thus is an important step in the implementation process.
- Requirement of clearly defined device-patient association workflows: Though the proposed method allows for flexibility in association workflows, the success and value of

this process is strongly linked to the quality, reliability, and efficiency of the association workflow used.

- Requirement of human involvement: Though the proposed method allows for the use of various technologies to assert device-patient associations, it is maintained that human verification at the point of care should always be included as an important part of such assertions.

5.4 Handling of Exception Cases

The following are examples of exception cases and their handling and are not intended to be exhaustive. This is an area for further development.

5.4.1 Conflict Detection and Handling

Depending on the details of implementation, there may be opportunities for cross-checking of device-patient association data from different sources. Any such opportunities should be sought out during system design and a user interface provided for asking to investigate and resolve the conflict. If the IHE PCD Alert Communications Management Profile is available, an alert message could be originated addressed to a clinician to alert them to the conflict, since the user interface might not get timely attention.

For example, an EMR system tracks the content of incoming Device Observation Reports it is receiving as IHE PCD-01 messages. If it receives data which is coming from a device that is not known to be associated with the patient identified in the observation report, it could request verification from the user that the device is in fact associated with the correct patient, and if this is confirmed the EMR could send a Device-Patient Association report to the manager.

5.4.2 One-click Override of known bad association

Provision should be made for a user to manually correct an association the user knows to be incorrect, rapidly.

5.4.3 Correction messages

When incorrect associations are detected and corrected, the Device-Patient Association Manager shall send corrected notifications to connected systems.

5.4.4 Use of time stamps to detect questionable associations

The Device-Patient Association Manager is expected to process association transactions relatively quickly, commensurate with expected end-user response times (generally one second or less). With this in mind, and to guarantee the integrity of the associations, this profile specifies the use of HL7 Application Level acknowledgments. This helps to ensure that the user of the association reporter (i.e., the person asserting the association) receives confirmation that the association manager is synchronized with the device.

A suspicious time lag in the flow of messages between actors can be an indication of inconsistent or doubtful data. If a Device-Patient association message from the Association Reporter is delayed getting to the Association Manager, then for a finite period of time, the Association

Reporter and the Association Manager are out of sync, thereby making the Device-patient association content of the Association Manager invalid. The Association Manager Device-patient association content ≠ Device-patient association state of the Association Reporter. Patient data from one device could be associated with the record of a different device. By limiting the process of establishing/ending device patient associations to well under the time it takes to physically remove one patient from the device and connecting a new patient, this scenario becomes remote.

5.4.5 System engineering considerations to ensure that the Device Patient Association Manager serves up accurate records:

- Specify HL7 application level acknowledgments.
- Retry if the device patient association manager does not acknowledge in a reasonable amount of time, maintaining original association timestamp.
- After a set number of retries, discontinue serving records of that specific device-patient association and assert alarm condition; reinitialize communications between Device-patient Association Reporter and Device-patient association manager

6 Next Steps

This document is being distributed for public comment (see description of the Public Comment process in Section 1.2). The drafting committee will carefully study the comments, determine if the comments warrant changes in the current edition of the document, a future revision of the document, or they are considered out of scope of the present process.

Then the work group, in consultation with the IHE PCD Technical Committee and Planning Committee, expects to use this document and the comments received in response to make a Profile Supplement for Trial Implementation with the intention of preparation of testable prototype implementations.

Appendix A – Proposed Messages

These message descriptions are not definitive; rather they are to give an idea of the approach and general expected content. Since they are rooted in the observation reporting messages of IHE PCD Device Enterprise Communications transaction PCD-01, refer to that profile in the current IHE PCD Technical Framework for details omitted here.

A.1 Report Device-Patient Association

As all of the use cases identified in this profile can be considered observations (it was observed that device d1 was connected to patient p1 starting at t1 and ending at t2), the ORU message structure is used throughout this profile to manage associations.

A.1.1 Message Structure

Appendix Table 1: Report Device Patient Association

Segments	Description
MSH	Message Header
[{ SFT }]	Software Segment
[UAC]	User Authentication Credential
PID	Patient Identification
[PV1]	Patient Visit Information (for room bed)
OBR	Observation Request
{	
OBX	Observation Result
{ PRT }	Participation
}	

MSH, SFT, and UAC Segments: Same as DEC Profile.

In the context of this use case, the message is constrained to reporting association(s) for a single patient. This could be single device, single patient, or multiple devices associated to a single patient.

A.1.2 Segments

A.1.2.1 MSH – Message Header

[DCP] We should designate MSH-9 and also decide if we want to specify application acknowledgments, or not, which must be declared in MSH as well.

A.1.2.2 PID – Patient Identification

In order to assert an association between a patient and a device, the PID segment is required. It identifies the patient who is associated to the device.

Appendix Table 2: PID Fields

SEQ	DT	OPT	RP	Description
1	SI	O		Set ID - PID
3	CX	R	Y	Patient Identifier List
5	XPN	O	Y	Patient Name
7	DTM	RE		Gender
8	IS	RE		DOB

860

A.1.2.3 PV1 Patient Visit Information

See IHE PCD-01 for basic information. In this profile, the PV1 segment is used to convey patient location information in PV1-3 Assigned Patient Location. This is also usable as a query filter to limit responses from the Device-Patient Association Query to matching locations.

865 ### A.1.2.4 OBR – Order Request

This segment serves as a wrapper for an association observation. It gives the association message a unique identifier in the Filler Order Number OBR-3. This acts as an association object instance identifier for tracking is used for tracking messages from all sources in the overall configuration of systems, so it must be constrained so that duplicate identifiers between sources are not
870 possible. It gives the timestamp of the association event.

A.1.2.5 OBX – Observation (for Patient ID)

This segment conveys the "observation" that the patient has been associated to a device. It includes the time stamp of the association event and the device ID. A PRT segment accompanies it to convey additional information about the device.

875

Appendix Table 3: OBX Fields

SEQ	DT	OPT	RP	Description
1	SI	O		Set ID - OBX
2	ID	R		Value Type – set to CWE
3	CWE	R		Observation Identifier – set to 68487^MDCX_ATTR_EVT_COND^MDC
4	ST	O		Observation Sub-ID. Use to convey a specific channel that's been associated, as <MDS>.<VMD>.<CHANNEL>.<facet>
5	CWE	R		Observation Value. See Appendix Table 4 - OBX-5 Values on page 30
11	ID	R		Observation Result Status. See Appendix Table 5 - OBX-11 Values on page 30.

Appendix Table 4: OBX-5 Values

Observation Value	Description
0^MDCX_DEV_ASSOCIATE^MDC	Device has been associated to a patient.
0^MDCX_DEV_DISASSOCIATE^MDC	Device has been disassociated from a patient.

A device association can be reported as a point-in-time event, in which case a separate disassociate message is required to delineate the end of the association. Alternatively, the association event message can convey a duration during which the association was in effect. The latter is equivalent to an associate/disassociate message pair, and may be preferable for short duration associations (e.g., spot vitals collection).

Appendix Table 5: OBX-11 Values

Status	HL7 Description	Adaptation
C	Record coming over is a correction and thus replaces a final result.	Record coming over is a correction and thus replaces a validated association.
D	Deletes the OBX record	Deletes the association record.
F	Final results; can only be changed with a corrected result.	Validated association. Can only be changed with a corrected association record.
R	Results entered -- not verified	An association has been asserted, but not validated.
W	Post original as wrong, e.g., transmitted for wrong patient.	Post original as wrong, e.g., transmitted for wrong patient.

A.1.2.6 PRT – Participation (Observation Participation)

This segment conveys information about persons and/or devices that participated in the association, ancillary to the patient and device that are its subjects. For example:

- A nurse that established and/or validated an association
- A device gateway
- The device itself, if the patient ID is entered directly onto the device

Appendix Table 6: PRT Fields

SEQ	DT	OPT	RP	Description
2	ID	R		Action Code. Always value to UC (unchanged).
4	CWE	R		Participation – see PRT-10 should contain some form of identifier sufficient to uniquely identify the device within the scope of the overall system. This is a repeating field, so more than one identifier can be given. See the discussion of OBX-18 in the IHE PCD Technical Framework Volume 2. If possible, it should have as one of its values the Unique Device Identifier defined by the US FDA, where applicable, but in any case must contain See details in the UDI Final Rule (U.S. Food and Drug Administration 2013) Appendix Table 7 - PRT-4 Values.
5	XCN		Y	Participation Person. If a person is the participant in this association message, his or her ID and name appear here.
9	PL		Y	Participation Location. Location where association was asserted or observed.
10	EI	C	Y	Participation Device. If a device is the initiator of this association record (PRT-4 = AUT), its ID appears here. Format is the same as in existing IHE PCD profiles and will match PRT-10 of device-as-subject PRT segment of this message, provided that the device associated with the patient and the device reporting the participation are one and the same (e.g., patient admitted on this monitor). If this PRT segment identifies this device as the subject of the association (PRT-4 = EQUIP), its ID appears here. Note – Prior to HL7 2.7, this would have appeared in OBX-18.
11	DTM	C		Participation Begin Date/Time (arrival time). Refer to Appendix Table 9 - PRT-12 Interpretation on page 33.
12	DTM	C		Participation End Date/Time (departure time). Refer to Appendix Table 8 - PRT-11 Interpretation on page 32.

895

PRT-10 should contain some form of identifier sufficient to uniquely identify the device within the scope of the overall system. This is a repeating field, so more than one identifier can be given. See the discussion of OBX-18 in the IHE PCD Technical Framework Volume 2. If possible, it should have as one of its values the Unique Device Identifier defined by the US FDA,
900 where applicable, but in any case must contain See details in the UDI Final Rule (U.S. Food and Drug Administration 2013)

Appendix Table 7: PRT-4 Values

Participation	HL7 Description	Adaptation
AUT	AUT Author/Event Initiator	The participant (nurse, device, etc.), initially asserts the association.
EQUIP	Equipment	The participant is the device that is a subject of the device-patient association.
RO	Responsible Observer	The participant (nurse, etc.) observes an already asserted association as a prelude to adjusting, validating, or marking in error.

905

Appendix Table 8: PRT-11 Interpretation

Participation Status	AUT	EQUIP	RO
R-Asserted	Time that the person/device asserted the association between the patient and device.	Time that the device-patient association is asserted to have been established.	Unusual. Time that the person in this role observed the person/device in the AUT role asserting the association.
C-Corrected	n/a	Corrected time that the device-patient association is asserted to have been established.	Time that the person in this role issued the correction.
D-Deleted	n/a	n/a	Time that the person in this role issued the deletion order.
F-Validated	n/a	Time that the device-patient association is confirmed to have been established. If null, most recently asserted/corrected time has been confirmed.	Time that the person in this role validated the association.
W-Wrong	n/a	n/a	Time that the person in this role declared the association to be erroneous.

Appendix Table 9: PRT-12 Interpretation

Participation → ↓Status	AUT	EQUIP	RO
R-Asserted	Time that the person/device asserted the disassociation between the patient and device.	Time that the device-patient disassociation is asserted to have taken place.	Unusual. Time that the person in this role observed the person/device in the AUT role asserting the disassociation.
C-Corrected	n/a	Corrected time that the device-patient association is asserted to have ended.	Time that the person in this role issued the correction.
D-Deleted	n/a	n/a	n/a
F-Validated	n/a	Time that the device-patient association is confirmed to have ended. If null, most recently asserted/corrected time has been confirmed.	Time that the person in this role validated the disassociation.
W-Wrong	n/a	n/a	n/a

A.2 Example Messages

Example 1: At 12:00, Nurse Diesel connected patient Spaniel to a continuous physiological monitor with ID MON5588. At 12:30, she records the association on the Critical Care application. As she is an RN and has witnessed and entered the association on the Critical Care system, this is considered a validated association. This message would be sent from the Critical Care system in the role of Association Reporter to the Association Manager.

```
MSH|^~\&|CritCare||AssocMgr||20160726123002||ORU^R01^ORU_R01|12d15a9|P|2.7|||AL|AL||88
59/1|||IHE PCD ORU-R01 2006^HL7^Universal ID^HL72390
PID|||AB60001^^^A^PI||Spaniel^C^R^^^^L
PV1||E|3 WEST ICU^3001^1
OBR|||15404652
OBX|1|CWE|68487^MDCX_ATTR_EVT_COND^MDC||0^MDCX_DEV_ASSOCIATE^MDC||||||F
PRT|1|UC||EQUIP||||||3 WEST ICU^3001^1|MON5588^^231A8456B1CB2366^EUI-64|20160726120000
PRT|2|UC||RO|58793^Diesel^N||||3 WEST ICU^3001^1||20160726123000
```

The Association Manager first responds with the following commit level acknowledgment.

```
MSH|^~\&|AssocMgr||CritCare||20160726123002||ACK^R01^ACK||P|2.7
MSA|CA|12d15a9
```

Once the association is fully processed, the Association Manager responds by initiating the following application level acknowledgment

```
MSH|^~\&|AssocMgr||CritCare||20160726123003||ACK^R01^ACK|AM52E123|P|2.7|||AL|NE||8859/
1|||IHE PCD ORU-R01 2006^HL7^Universal ID^HL72390
MSA|AA|12d15a9
```

To which the Association Reporter responds with a commit level acknowledgement, completing the exchange.

```
MSH|^~\&|CritCare||AssocMgr||20160726123003||ACK^R01^ACK||P|2.7
MSA|CA|AM52E123
```

Example 2: At 16:00, Nurse Ratched connected patient McMurphy to a continuous physiological monitor with ID MON5596. She enters his patient ID on the monitor and presses a button causing the association to be asserted.

```
MSH|^~\&|MonitorGateway||AssocMgr||20160726160000||ORU^R01^ORU_R01|12d1574|P|2.7|||AL|
AL||8859/1|||IHE PCD ORU-R01 2006^HL7^Universal ID^HL72390
PID|||AB60001^^^A^PI||McMurphy^R^P^^^^L
PV1||E|3 WEST ICU^3001^1
OBR|||15404697
OBX|1|CWE|68487^MDCX_ATTR_EVT_COND^MDC||0^MDCX_DEV_ASSOCIATE^MDC||||||R
PRT|1|UC||EQUIP||||||3 WEST ICU^3001^1|MON5588^^231A8456B1CB2366^EUI-64|20160726160000
PRT|1|UC||AUT||||||3 WEST ICU^3001^1|MON5588^^231A8456B1CB2366^EUI-64|20160726160000

(Acknowledgment messages not shown)
```

The Association Manager may then broadcast this information to subscribers (such as Critical Care), or its clients (such as Critical Care) may query for this information, depending on how the systems are integrated.

At 16:45, she confirms the association on the Critical Care application (or the Association Manager, depending on how the systems are integrated). This message would be sent from the Critical Care system in the role of Association Reporter to the Association Manager.

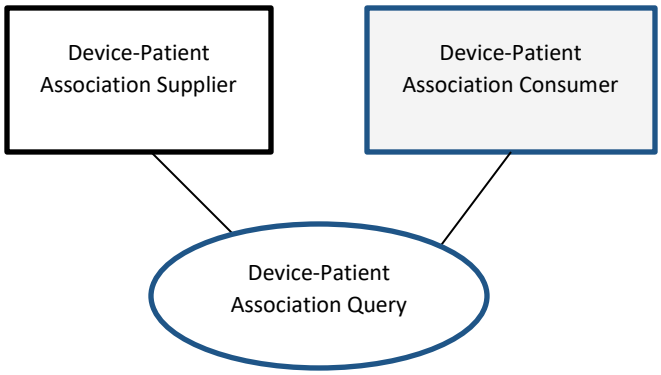
```
MSH|^~\&|CritCare||AssocMgr||20160726164500||ORU^R01^ORU_R01|12d1574|P|2.7|||AL|AL||88
59/1|||IHE PCD ORU-R01 2006^HL7^Universal ID^HL72390
PID|||AB60001^^^A^PI|| McMurphy^R^P^^^^L
PV1||E|3 WEST ICU^3001^1
OBR|||15404697
OBX|1|CWE|68487^MDCX_ATTR_EVT_COND^MDC||0^MDCX_DEV_ASSOCIATE^MDC||||||F
PRT|1|UC||EQUIP||||||3 WEST ICU^3001^1|MON5588^^231A8456B1CB2366^EUI-64|20160726160000
PRT|2|UC||RO|58787^Ratched^N||||3 WEST ICU^3001^1||20160726164500

(Acknowledgment messages not shown)
```

A.3 Query: Device-Patient Associations Query Message

A.3.1 Scope

This query allows a system to request a list of the device-patient associations meeting specified conditions.

A.3.2 Use Case Roles



A.3.3 Query Message

QBP	Query by Parameter	Chapter in HL7 2.5
MSH	Message Header	2
QPD	Query Parameter Definition	5
RCP	Response Control Parameter	5
[DSC]	Continuation Pointer	2

A.3.3.1 MSH Segment

As for transaction PCD-01 in the IHE PCD Technical Framework.

A.3.3.2 QPD Segment

QPD - Query Parameter Definition

Mnemonic	Description	Type	Optionality	Length	Table	Repetition
QPD.1	Message Query Name	CE	Required	250	471	No
QPD.2	Query Tag	ST	Optional	32		No
QPD.3	User Parameters	VARIES	Optional	256		No
QPD.4	Action Code	ID			323	

The User Parameters field (QPD.3) is used to specify "filtering" values, so that the query response can be limited to, for example, the records matching a particular Patient Identifier (by

including a PID.3 specification), a particular device (by adding a Participation Device PRT specification) and so on. If multiple specifications are given, the responding system "AND"s the specifications together, so that for example, a patient identifier and a device identifier specification result in the response only gives associations involving that patient and device.

The Action Code (QPD.4) is used if a subscription is being modified (specified in RCP-5), and has the value A if a subscription is being added or D if it is being deleted

The form of the specifications in QPD field follows the conventions established by the ITI Patient Data Query Profile (ITI-21, see the ITI Technical Framework, Vol. 2a): one or more repetitions (separated by the HL7 repetition separator, by default the tilde character ~), with each repetition in the form of subcomponent specifying the field, component, or subcomponent to filter on as @<seg>.<field number> followed by a subcomponent giving the value sought for that field. (It's simpler than it sounds: an example would be:

```
@PID.3.1^MR123~@PRT.10^PUMP1
```

Meaning limit segments given in response to ones involving patient identifier MR123 and device identifier PUMP1.

FLD	ELEMENT NAME
PID.3	Patient Identifier List
PV1.3	Assigned Patient Location
PRT.10	Participation Device

A.3.3.3 RCP Segment

RCP - Response Control Parameter

Field	Description	Type	Optionality	Length	Table	Repetition
1	Query Priority	ID	R	1	91	No
2	Query Limited Request		X			
3	Response Modality	CNE				
4	Execution and Deliver Time					
5	Modify Indicatory	ID				

The possible values for RCP-1, Query Priority, are:

Value	Description	Comment
D	Deferred	
I	Immediate	

"Immediate" mode corresponds to a "one-shot" information request. "Deferred" mode can specify a persistent "subscription" to events matching the query specification.

Quantity limited requests are not supported, so RCP-2 Quantity Limited Request value is not used.

The supported values of RCP-3 Response Modality are R (Real Time) or T (Bolus)

RCP-4 Execution and Delivery Time is required when RCP-1 contains the value of RCP-1 D (Deferred). It specifies when the response is to be returned. It can be used in a subscription to give a future time when a subscription is to be terminated.

RCP-5 Modify Indicator specifies whether a new subscription is being requested (value: N), or a modification is being made to an existing subscription (M). QPD-4 Action Code can signify the deletion of a subscription with a value of D.

A.4 Query Response Message

RSP	Segment Pattern Response
MSH	Message Header
MSA	Message Acknowledgement
[{ERR}]	Error
QAK	Query Acknowledgement
QPD	Query Parameter Definition
{	--- Association Begin
PID	Patient Identification
[PV1]	Patient Visit Information (for room bed)
OBR	Observation
OBX	Observation (for Patient ID)
{ PRT }	Participation (Observation Participation)
}	--- Association End

A.4.1 MSH Segment

As for transaction PCD-01 in the IHE PCD Technical Framework.

A.4.2 MSA Segment

As for the generic HL7 QSB query

A.4.3 QAK Segment

The QAK segment gives a query tag identifying the particular query instance, for tracking

SEQ	LEN	DT	OPT	TBL#	ELEMENT NAME
1	32	ST	R		Query Tag
2	2	ID	R+	0208	Query Response Status

A.4.4 QPD Segment

The query response simply echoes the QPD segment from the query here.

A.4.5 Remaining Segments

The remaining segments in the segment pattern correspond to any associations matching the query specification.

Appendix B – Use Cases from HL7 Detailed Clinical Models for Medical Devices

B.1 Associate the Medical Device with a Patient by Identifier and Point-of-Care

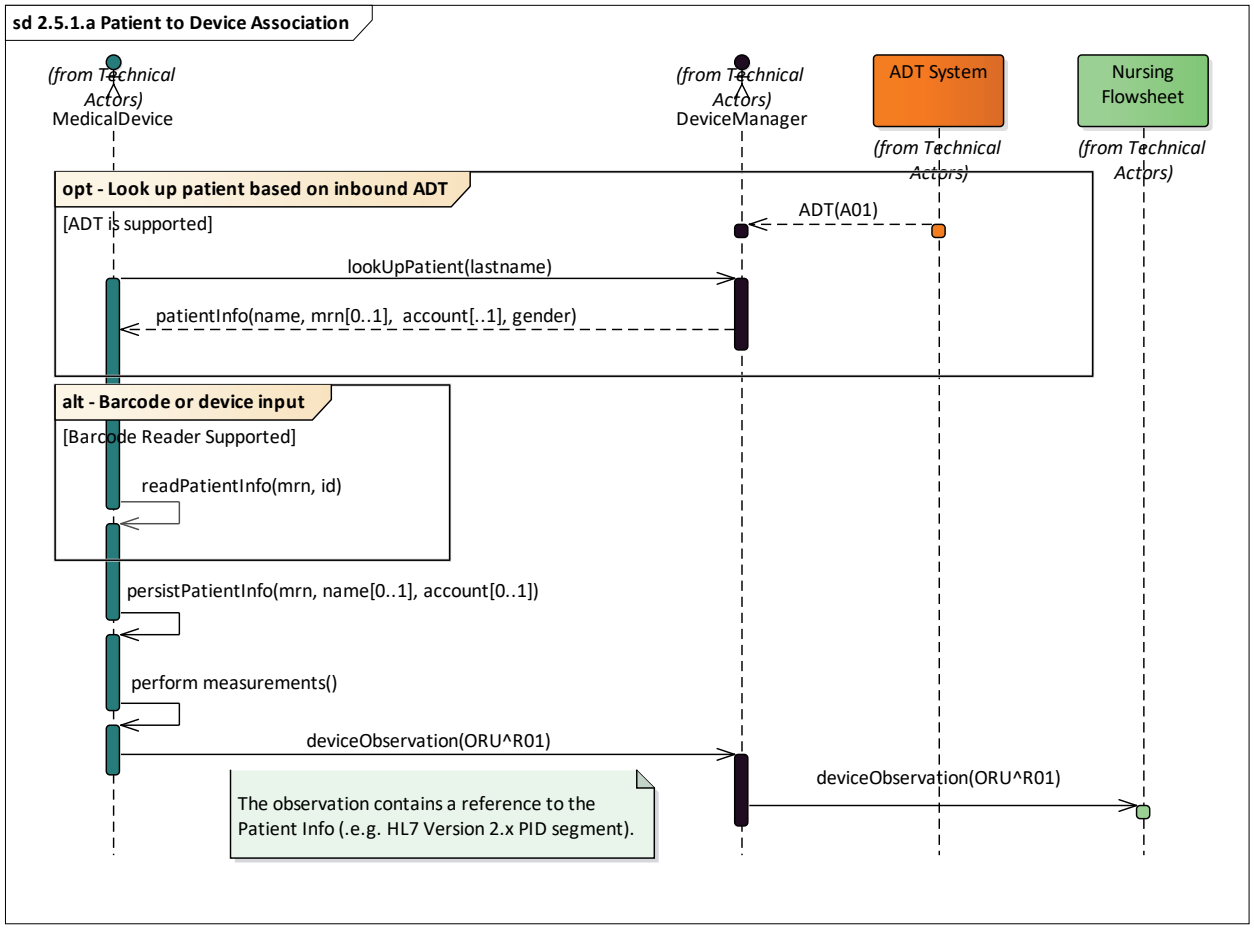
Both location and patient's identifier are used to determine whether the device should be associated with a specific location.

The operator scans or enters the patient's identity into the device using its user interface, bar code reader, etc.

The device is used to treat or monitor the patient's condition.

Once the device is no longer needed, the operator discontinues the association. This removes the patient's identity from the data produced by the device.

When the device is no longer acquiring data for the patient, the association with the medical device is broken. In some cases, the data may need to be validated by a clinician (e.g., nurse) before it is permanently committed to the patient's record.



B.2 Associate the Medical Device with a Patient by Selecting Patient on Device

This use case is applicable in highly integrated environments. It requires an encounter management system (ADT) integrated either with the device directly or through its Medical Device Manager or an Order Entry System.

The identity may be established indirectly through an order number (e.g., accession number, placer order number) that is used by the device to reference its measurement.

The association may need to be confirmed by end-users.

B.2.1 Pre-Conditions

The device or its device manager is tracking encounter events (e.g., admission) or queries its Device Manager for patients as needed.

B.2.1.1 Main Scenario

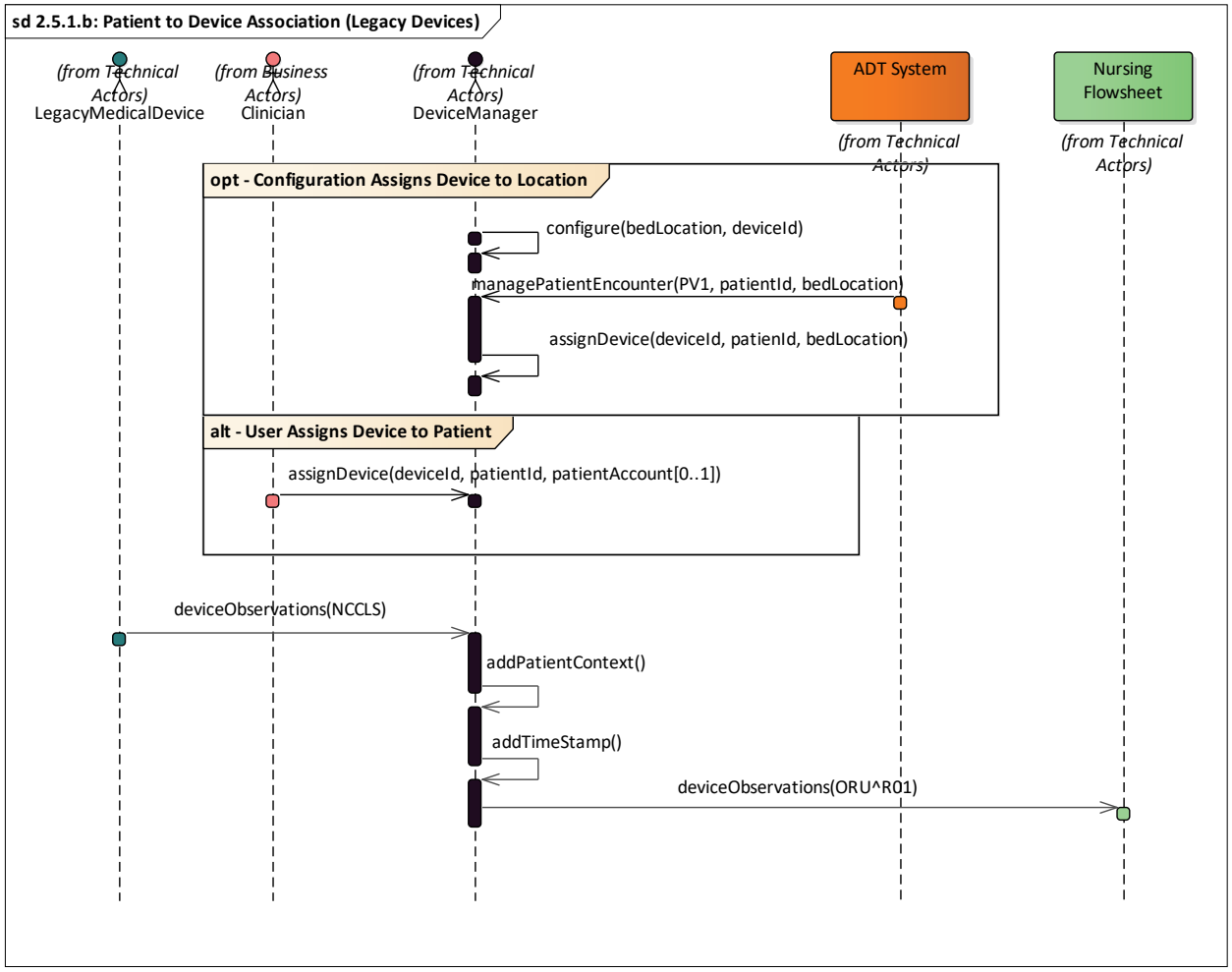
The operator enters a set of patient identifier traits into the medical device to loop up the patient's identity.

The operator selects the appropriate patient record and associates the device with the patient.

When the device is disconnected from the patient, the association is automatically broken.

B.2.2 Post-Conditions

The information reported by the device while the device was associated with the patient is charted to the patient's record. In some cases, the data may need to be validated by a clinician (e.g., nurse, respiratory therapist) before it is permanently committed to the patient's record.



B.3 Associate the Medical Device with a Patient by Patient Identifier Only

This use cases provides the most efficient patient-to-device association provided that the patient's identifier is entered correctly into the device.

B.3.1 Pre-Conditions

The device is able to record the patient's identity.

B.3.2 Main Scenario

The Medical Device Operator enter the patient's identity using the device input device (e.g., keyboard, bar code scanner). The precision with which the patient's identifier is entered into the device determines how accurate the association between the patient and device is, and consequently, how accurate the patient identity component of the output data is.

B.3.3 Post-Conditions

The information is received by the destination information system or EHR-System and associated with the patient identified by their patient identifier. In some cases, the data may need to be validated by a clinician (e.g., nurse) before it is permanently committed to the patient's record.

Appendix C – Security Considerations in the Use of This Proposed Profile

This profile itself does not impose specific requirements for authentication, encryption, or auditing, leaving these matters to site-specific policy or agreement. The IHE PCD Technical Framework identifies security requirements across all PCD profiles.

To assist the user of this profile with security considerations, a non-exhaustive exemplar of a security risk table is presented below:

C.1 General IHE PCD Guidance

During the profile development there were no unusual security/privacy concerns identified. There are no mandatory security controls, but the implementer is encouraged to use of the underlying security and privacy profiles from ITI that are appropriate to the transports, such as the Audit Trail and Node Authentication (ATNA) Profile. The operational environment risk assessment, following ISO 80001, will determine the actual security and safety controls employed.

C.1.1 Risk Assessment and Mitigation for Proposed Device-Patient Association Profile

The following content is to provide a non-exhaustive treatment of potential security risks for consideration. The implementer is strongly encouraged to take such risks into account in the actual development and deployment of this profile.

Characterization of risks			Assessment of risks		Mitigation of risks		
Scenario	**Asset**	**Type of Impact**	**Level of Impact**	**Probability**	**Mitigation**	**New Level of Impact**	**New Probability**
Attack on Device-Patient Association Manager	Device IDs	Attacker compromises Device ID, leading to unreliable information in the EHR.	Very High	High	ITI EUA	Very High	Medium
	Patient IDs	Attacker compromises Patient ID, leading to unreliable information in the EHR.	Very High	Medium	ITI ATNA	Very High	Low
	Binding Table	Attacker corrupts Binding Table, leading to unreliable information in the EHR.	Very High	Medium	ITI DEN	Very High	Low
Attack on Device-Patient Association Reporter	Device IDs	Attacker compromises Device ID, leading to mis-assignment of device identity in the EHR.	Very High	High	ITI EUA	Very High	Medium
	Patient IDs	Attacker compromises Patient ID, leading to mis-assignment of patient identity in the EHR.	Very High	Medium	ITI ATNA	Very High	Low

Characterization of risks			Assessment of risks		Mitigation of risks		
Scenario	**Asset**	**Type of Impact**	**Level of Impact**	**Probability**	**Mitigation**	**New Level of Impact**	**New Probability**
	Patient Data	Attacker reads patient data, leading to compromise of patient privacy.	Medium	Medium	ITI DEN	Medium	Low
Attack on Device-Patient Association Consumer	Device-Patient Association	Attacker compromises Device-Patient Association, leading to delayed or no availability of Device-Patient Association information.	Very High	High	ITI DEN	Very High	Medium
Attack on Device Registrant	Available Devices (Device IDs)	Attacker compromises Device ID, leading to mis-assignment of device identity in the EHR.	Very High	High	ITI EUA	Very High	Medium

C.2 Implications of the Security Risk Analysis

1. User authentication is needed for actors which either provide or consume the patient-device binding information.
2. Patient-device binding tables should require similar credentials for authorized access.
3. Transport of patient-device binding information should be encrypted to assure integrity and confidentiality of its contents.

There are several security profiles from IHE ITI domain that can be useful in supporting security control measures indicated by the Security Risk Analysis. For example:

1. ITI ATNA (Audit Trail and Node Authentication) Integration Profile can provide confidentiality, data integrity, and user accountability for accesses to the patient-device binding table. This profile can be used for user authentication to the Device-Patient

Association Manager. This profile can also be used to create an audit trail of accesses to the Device-Patient Association Manager.

2. ITI EUA (Enterprise Authentication) may be used for actors which seek to authenticate themselves with the Device-Patient Association Manager.
3. ITI DEN (Document Encryption) Integration Profile may be used to encrypt the transport of patient-device binding table information.

Due to the severity of impact of a security breach, implementers of the Device-Patient Binding Integration Profile are strongly urged to take precautionary steps with regard to security considerations.

Security Risk Assessment and Mitigation for Proposed Device-Patient Association Profile

Attack on Device-Patient Association Manager: use of ITI EAU to avoid compromise of Device IDs that are sent to the EHR.

Attack on Device-Patient Association Manager: use ITI ATNA to avoid compromise of Patient IDs that are sent to the EHR.

Attack on Device-Patient Association Manager: use of ITI DSG to avoid corruption of Binding Table.

Attack on Device-Patient Association Consumer: use of ITI XUA to enhance Device-Patient Association availability.

Resources that are available from IHE ITI

Definitions

ITI EAU

http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Vol1.pdf

Enterprise User Authentication: defines a means to establish one name per user that can then be used on all of the devices and software that participate in this integration profile. It greatly facilitates centralized user authentication management and provides users with the convenience and speed of a single sign-on. User authentication is a necessary step for most application and data access operations and streamlines workflow for users.

ITI ATNA

http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Vol1.pdf

Audit Trail and Node Authentication (ATNA): establishes the characteristics of a Basic Secure Node:

It describes the security environment (user identification, authentication, authorization, access control, etc.) assumed for the node so that security reviewers may decide whether this matches their environments.

It defines basic auditing requirements for the node.

It defines basic security requirements for the communications of the node using TLS or equivalent functionality.

http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Vol2a.pdf

ITI DSG

http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Vol1.pdf

The Cross-enterprise Document Media Interchange (XDM) Integration Profile may be used in conjunction with the DSG Integration Profile to provide for the digital signature of the 7515 documents content and of the XDS metadata.

ITI XUA

http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Vol1.pdf

Cross-Enterprise User Assertion (XUA) provides a means to communicate claims about the identity of an authenticated principal (user, application, system...) in transactions that cross-enterprise boundaries. To provide accountability in these cross enterprise transactions there is a need to identify the requesting principal in a way that enables the receiver to make access decisions and generate the proper audit entries. The XUA Profile supports enterprises that have chosen to have their own user directory with their own unique method of authenticating the users, as well as others that may have chosen to use a third party to perform the authentication.

Rationale for Application

ITI EAU can be implemented to enable authentication between Device-Patient Association Manager and other actors. Without such authentication, the Device-Patient Association Manager will not communicate with the EHR. Device IDs will only be exchanged by authenticated partners.

ITI ATNA can be implemented to facilitate secure communications between actors. Using ITI ATNA, Patient IDs can be exchanged between EHR and Device-Patient Manager.

Appendix D – Glossary

Assertion

A statement that a certain premise is true.

Device-Patient Association Consumer

A system or person that queries a Device-Patient Association Manager for device-patient association records.

Device-Patient Association Manager

A system that records, manages, and serves records of device-patient associations.

Association Reporter

A system or person that asserts a device-patient association, disassociation, or attributes related to either.

Binding

A process of associating two related elements of information.

Biometrics

A measurable physical characteristic or personal behavioral trait used to recognize the identity, or verify the claimed identity of a person.

Device-Patient Association

A link between a patient identity and one device identity that is established on the basis of evidence. It has a start time and, once it is no longer active, an end time.

Device Registrant

A system (including the device itself) or person that identifies a device that may participate in device-patient associations.

Device Registration System

A system that identifies patients that may participate in device-patient associations.

Direct Association

A patient association established by the observation and recording of a physical connection of a device to the patient.

Direct Device-Patient Association Assertion

A claim of direct device-patient association based on evidence.

Duplicate Patient Identification Record

Two records representing the same patient, with differing identifiers of the same type with the same assigning authority. For example, two different medical record numbers issued by the same hospital to the same patient. In the context of device-patient association, an unintentional duplicate patient record may result if device data is recorded without a permanent unique patient

identifier being recorded, as in an emergency. A human-validated merge operation is necessary to associate the device data with the patient after the fact.

Entity

An organizational unit within a healthcare enterprise, typically, but not necessarily, associated with a free-standing building, office, or sub-unit within a common hospital corporation. For example, a patient visit would occur within a specific entity.

False Negative

Patient algorithm matching error occurring when two different records for the same person are thought to represent different people (for example name, gender, date of birth, MRN…).

False Positive

Patient algorithm matching error occurring when information for two different people appears to be a match representing the same individual (for example name, gender, date of birth, MRN…).

Identity Assertion

A claim attributing a particular identity to a person or device.

Identity Management

Identity management (IdM) is composed of the set of business processes, and a supporting infrastructure, for the creation, maintenance, and use of digital identities within a legal and policy context.

Indirect Device-Patient Association

A patient association asserted on the basis of a common attribute shared by a device and patient, such as a location.

Location-based Assertion

An assertion of an association between two objects (e.g., a patient and a device, device-to-device, patient-to-caregiver), based solely upon the co-location (e.g., same room and bed) of these two objects.

Minimal Guarantee

The fewest promises the system makes to its stakeholders, particularly when the primary actor's goal cannot be delivered.

Multi-Entity

A healthcare enterprise consisting of two or more entities. For example, a hospital corporation which owns three hospitals.

Observation-Patient Association

The assignment of a device measurement/parameter to a specific patient. Observation - patient associations are established through the connection relationship of a unique patient to a unique device at the point in time that the measurement was recorded by the device.

Overlap Record

One person with two or more unique enterprise identifiers. Without the two records being linked, information not available for point of care and clinical decisions are made in the absence of data. There is an increase in costs associated with repeat test, clinical procedures, etc., as well as rework in clinical and business processes.

Overlay Record

Records of two different people are "combined" into one record in error. Person A is treated with Person B's clinical information. This has huge implications for quality of care and patient safety.

Device-Patient Association Query

A request to a system whereby patient and/or device identifiers are provided, with the response composed of matching device-patient associations.

Device-Patient Association Conflict Notification

A message from a particular clinical IT system that it detects an inconsistency between different identity assertions. For example, a device and an intermediary system may be simultaneously asserting that a single data stream represents two different patients.

Device-Patient Record Linkage

The process of binding and/or associating a discrete patient record to a discrete device record.

Patient Identity Binding

The process of attaching a probabilistically selected identity to health records for a person whose identity has not been fully established.

Patient Identity Management

Patient identity management (PIM) has been defined as the "ability to ascertain a distinct, unique identity for an individual (a patient), as expressed by an identifier that is unique within the scope of the exchange network, given characteristics about that individual such as his or her name, date of birth, gender [etc.]." The scope of this definition can be expanded to refer to PIM as the process of accurately and appropriately identifying, tracking, managing, and linking individual patients and their digitized health care information, often within and across multiple electronic systems.

Patient Index (Master Patient Index)

A system, typically centralized for a provider institution or organization, which is authoritative for patient demographic information including identity data, for patients under care. Typically can respond to queries and give a unique identity or a set of candidate identities that are consistent with a set of identity factors.

Patient Linkage

The general problem of determining whether two existing records pertain to the same patient. This is distinct from device-patient association and uses different methods.

Patient Matching

Record linkage is the task of identifying pieces of scattered information that refer to the same thing. Patient matching is a specific application, in which we try to identify records that belong to the same patient among different data sources.

Precondition

"What the system under analysis will ensure is true before letting the use case start."

Proofing (Identity Proofing)

The process of collecting and verifying sufficient information (e.g., identity history, credentials, documents) from an applicant to a service provider for the purpose of proving that a person or object is the same person or object it claims to be.

Receiving System

In the context of PCIM, any system which is a consumer of device-patient association or observation messages, such as an electronic medical record system, device gateway, or a device at the point of care.

Record

The discrete representation of a specific and unique patient or the device in either the reporting or consuming system's database.

Strong Identity Assertion

A presumption of patient or device unique recognition using multiple factors that provides a high degree of accuracy and certainty (e.g., barcode, biometric).

Strong Identity Factors

An identifier designed to be unique (applies to only one person) and consistent over the appropriate domain for at least throughout the visit or encounter, for example, Medical Record Number or National ID number.

Success Guarantee

A success guarantee is a statement of what interests of the stakeholders are satisfied after a successful conclusion of the use case.

Unique Device Identifier

In the US, a unique identifier for a medical device that is recognized by the US FDA and which has a part that identifies the maker and model of the device (DI) and a part that identifies the particular instance of the device. More generally, any identifier which allows a particular device to be uniquely identified.

Weak Identity Assertion

A presumption of patient or device unique recognition using factors that provides a low degree of accuracy and certainty (e.g., name, location).

Weak Identity Factors

Factors which can contribute to identification, but typically are not unique to patient; for example, name, sex, date of birth.

Appendix E – References

ECRI Institute. 2013a. 'Safety risks of electronic health records', *Health Devices*, 42: 134-5.
1345 ———. 2013b. 'Top 10 health technology

hazards for 2014', *Health Devices*, 42.
———. 2015. "Top 10 Health Technology Hazards for 2015." In. https://www.ecri.org/EmailResources/PSRQ/Top10/2015_Patient_Safety_Top10.pdf
ECRI Institute Patient Safety Organization. 2012. 'ECRI Institute PSO Deep Dive: Health
1350 Information Technology--Toolkit'. https://www.ecri.org/components/PSOCore/Documents/Deep%20Dive/Deep%20Dive%20-%20HIT%20Toolkit%200113.pdf

Frisch, P., S. Miodownik, P. Booth, P. Carragee, and M. Dowling. 2009. 'Patient centric identification and association', *Conf Proc IEEE Eng Med Biol Soc*, 2009: 1722-5.
1355 HIMSS Patient Identity Integrity Work Group. 2009. 'Patient Identity Integrity': 60. http://www.himss.org/files/HIMSSorg/content/files/PrivacySecurity/PIIWhitePaper.pdf

EC. 2009. "IEC TR 80002-1, Medical device software — Part 1: Guidance on the application of ISO 14971 to medical device software." In *IEC TR 80002-1*.
———. 2010. "Application of risk management for IT-networks incorporating medical devices -
1360 - Part 1: Roles, responsibilities and activities." In *IEC Standard 80001-1*. C:\Data\Protocols\AAMI\ITn17.pdf
ISO. 2007. "ISO 14971, Medical devices -- Application of risk management to medical devices." In.
Melendez, Luis. 2012. 'Integrating patient data: safety concerns limit functionality', *Biomed*
1365 *Instrum Technol*, 46: 64-7. http://www.ncbi.nlm.nih.gov/pubmed/22239365
———. 2014. *Compendium: Medical Device Integration and Informatics* (AAMI).
NorthPage Research. 2010. '5 tips for successful patient identity management in government agencies.'. http://www.govhealthit.com/sites/govhealthit.com/files/resource-media/pdf/northpagereportpatientidentitymanagementtipsforgovtagencies.pdf

1370
Office of the National Coordinator for Health Information Technology. 2014. 'Patient Identification and matching final report'. https://www.healthit.gov/sites/default/files/patient_identification_matching_final_report.pdf.
1375 Singureanu, Ioana. 2015. "Detailed Clinical Models for Medical Devices." In. http://www.hl7.org/implement/standards/product_brief.cfm?product_id=392

http://wiki.hl7.org/index.php?title=Detailed_Clinical_Models_for_Medical_Devices
U.S. Food and Drug Administration. 2013. 'Unique Device Identification System. Final Rule.'. https://www.federalregister.gov/articles/2013/09/24/2013-23059/unique-device-
1380 identification-system

———. 2015. 'Food and Drug Administration Modernization Act of 1997:

Modifications to the List of Recognized Standards, Recognition List '. https://www.gpo.gov/fdsys/pkg/FR-2015-08-14/html/2015-19991.htm

Zaleski, John. 2015. *Connected Medical Devices: Integrating Patient Care Data in Healthcare Systems* (HIMSS).

