Secure and Reliable Data Exchange with Devices

February 21, 2017

Amit Trivedi, Program Manager - Healthcare

ICSA Labs
Speaker Introduction

Amit Trivedi
Program Manager, Healthcare
ICSA Labs
Agenda

• ConCert by HIMSS Certification – Program Overview
• New for 2017: ConCert Approved Medical Devices
• Next Steps and the ConCert 2018 Cycle
• Q/A
Certified Connectivity. Finely Tuned Simplicity.
Program Overview

- ConCert by HIMSS™ is a comprehensive interoperability testing and certification program administered by ICSA Labs, governed by HIMSS, and built on the work of the EHR | HIE Interoperability Workgroup and IHE USA.

- Certification targets HIT solutions that facilitate standards-based, secure, and reliable data exchange.

- Leverages both ISO/IEC 17025 (testing) and 17065 (certification) accreditation requirements to ensure industry recognition and program rigor.

The only vendor-independent certification that assures providers that products are interoperable and is backed by trusted industry leaders.
Value of Certification to Healthcare Industry

Care Providers

• Simplify purchase decisions by enabling objective evaluation of device-connectivity solutions
• Transparent and collaborative process and commitment supporting the evolution of reliable, interoperable solutions

Health IT Product Companies

• Only private-sector, standards-based ISO-accredited level of testing and certification program; reciprocity opportunities with other testing/certification programs
• Improves return on interface development time/cost; reduction in custom solutions
• Reduces implementation time/cost at customer installations
- Patient identification
- Secure point-to-point messaging
- Retrieve documents
- Provider queries

- Patient identification
- Document exchange
- Communicate with HIEs in other communities

- Provider information exchange
- Secure point-to-point messaging
Going Beyond the Minimum Requirements

**ONC Health IT**

170.315(e)(1) View, Download, and Transmit

Limited to only portions of e1 that utilize Direct XDR

170.315(e)(2) Secure Messaging

Direct SMTP only

ConCert tests back-end transactions whereas ONC tests front-facing messaging

**ConCert by HIMSS™**

- Direct SMTP (with XDM)
- Direct XDR
- HPD Consumer
- HPD Directory
- PDQ Consumer
- PDQ Supplier
- PIX Consumer
- PIX Patient Source
- PIX Manager
- XCA Gateway
- XDS Document Source
- XDS Document Consumer
- XDS Registry
- XDS Repository
Designed to be Complementary

• Very little overlap between the programs, demonstrating that they complement each other

• ConCert builds upon and goes beyond meaningful use

• ConCert focuses on interoperability *between* disparate information systems whereas ONC Health IT Certification allows for similar functionality directly within the *same* system
Interoperability Testing Tool (ITT)

- Designed from the outset for use by both a testing lab and a certification body organization
- Cloud-based, automated, self-service tool
- Individual test cases, or group-based testing
- Practice or Certification modes
- All necessary information at your fingertips (SUT, ITT, test cases, specifications, etc.)
- Test results – detail and summary
- Detailed troubleshooting help with references to underlying specifications
ITT – Architecture Overview

ITT Web UI
- User Mgt.
- SUT Mgt.
- Test Results Mgt.
- Test Case Mgt.
- Test Execution

ITT API

ITT Data
- Config.
- SUT
- User
- Test Case
- Test Result
- Logs

ITT Test Execution Controller

Test Tool Adapters
- SOAP
- HL7
- Direct
- Other Testing Tools

Add New Certification Testing Module

Data Access

Test Invocation

Testing Tools
- SOAP Testing Tools
- HL7 Testing Tools
- Direct Testing Tools
- Other Testing Tools
New for 2017: ConCert Approved Medical Device

Certification Marks signify compliance and proof that a product has all of the requirements to be interoperable with other certified ConCert by HIMSS products.

for medical devices and EHR systems to provide a standardized way to exchange programming order information and clinical information at the point of care.
Testing Tools and Methodology Based on IHE-CAS

IHE CONFORMITY ASSESSMENT
Industry leaders collaborating to deliver production ready, secure, and interoperable Electronic Health Records (EHRs), Health Information Exchanges (HIEs), Health Information Service Providers (HISP), and Patient Care Devices.

Integrating the Health Care Enterprise – IHE International
IHE is an initiative by healthcare professionals and industry to improve the way healthcare information systems share information. IHE promotes the coordinated use of established standards such as DICOM and HL7 to address specific clinical needs in support of optimal patient care.

ICSA Labs, an independent division of Verizon, represents IHE USA and the US region as the authorized testing lab for the Conformity Assessment Program.
IHE PCD Actor Profiles Tested

• **Device Observation Reporter (DOR)** = Evaluates the capability to transmit valid PCD-01 messages to a DOC and consume the ACKs. Includes validation of Pulse Oximetry Integration messages.

• **Device Observation Consumer (DOC)** = Evaluates the capability to consume valid PCD-01 messages from a DOR and transmit the Accept ACKs. Includes validation of Pulse Oximetry Integration messages.

• **Infusion Order Programmer** = Evaluates the capability to transmit valid PCD-03 messages to a IOC and consume the Application Acknowledgement messages.

• **Infusion Order Consumer** = Evaluates the capability to receive valid PCD-03 messages from an IOP and transmit the Application Acknowledgement messages.
Grounded in IHE PCD Transactions

- HL7 v2.x message types
- DEC: Test data is supported from periodic, near-periodic and infrequent senders
- PIV: Test data is supported from LVP, PCA, and Syringe Type Pumps
- DEC/PIV: Test data tailored to specific characteristics of system under test, e.g.
  - e.g. Bedside monitors will support heart rate, blood pressure (systolic, diastolic, mean, etc)
IHE PCD-DEC Profile (Device to Enterprise Communications)

The PCD-DEC (Device to Enterprise Communications) profile allows a consuming system (DOC) to receive patient clinical information including vitals, demographics, settings, and location from a reporting device/system (DOR).

*Slide Content developed by IHE and the PCD Technical Committee
The **PCD-PIV** (Point-of-Care Infusion Verification) profile supports the electronic transfer of infusion parameters from a Bedside Computer-assisted Medication Administration (BCMA) system or EMR to a general-purpose infusion pump, enhancing patient safety by effectively eliminating keystroke errors.

*Slide Content developed by IHE and the PCD Technical Committee*
ConCert Medical Device Certification Pilot

2017 Pilot Participants

- BD
- BRAUN
- Baxter
More Devices are Being Connected Every Day

We can take industry best practices, guidance, and recommendations and use that as a basis to create minimum requirements for functionality, interoperability, and increasingly more important – privacy and security.
Medical Devices, IoT and Cyber Security

In healthcare – insecure medical devices are a mounting concern:

• Implantable Cardioverter Defibrillators (ICD)
• Insulin Pump
• Drug infusion pumps
• X Ray systems / centralized storage
• Blood refrigeration Units
• CT Scanning equipment
• Remote monitoring systems
• Clinical Data Repositories
Fundamental differences in priorities lead to challenges addressing security

• Traditional IT security postures often describe priorities using the acronym C-I-A. Confidentiality – Integrity – Availability.

• In the healthcare environment, which reflects a different nature of mission and business critical function, taking patient safety as a paramount concern - the priorities are reversed: **Availability – Integrity – Confidentiality**.

• This is reflected in the hospital-internal processes and priorities, such as the different job functions of IT and Biomedical Engineering, and it also results in very different regulatory frameworks and guidance.
FTC: Recommendations

• FTC Report on Internet of Things urges companies to adopt best practices to address privacy and security risks.
• Report recognizes that the rapid growth of connected devices offers societal benefits, but also risks that could undermine consumer confidence.
Guidance and recommendations

Medical Equipment Management (MEM): Medical Device Cyber Security – Best Practice Guide (Draft)
IHE PCD in Cooperation with MDISS White Paper: Medical Device Patching

- How today’s medical devices are used and incorporated in our IT environments.
- What type of cyber-threats they are exposed to and how these threats can affect the medical device ecosystem.
- A review of best practices to design security into medical devices and reliable medical device networks, ranging from asset and configuration management access control, to cyber-security protective measures.
Guidance and recommendations

HIPAA
HITECH
FDA:
• 21 CFR 801, 803, 807, 812, 814, 820
• Cybersecurity Guidance
IEC 80001
IHE PCD
MDS²
Joint Commission:
• EC.02.04.01

Figure 1: The Complexities of Medical Device Security
Guidance and recommendations

Medical Equipment Management (MEM): Medical Device Cyber Security – Best Practice Guide (Draft)
IHE PCD in Cooperation with MDISS White Paper: Medical Device Patching

• How today’s medical devices are used and incorporated in our IT environments.
• What type of cyber-threats they are exposed to and how these threats can affect the medical device ecosystem.
• A review of best practices to design security into medical devices and reliable medical device networks, ranging from asset and configuration management access control, to cyber-security protective measures.
ConCert by HIMSS Roadmap & Next Steps

- Pilot testing will validate the new set of tools and interoperability requirements.
- Pilot participants will be encouraged to provide input on the ConCert 2018 cycle
  - Cyber security-centered certification testing
  - Capabilities to test a wide range of IoT devices & sensors
- Targeting device and its component parts
  - Requirements derived from a 6-category IoT Framework
  - Can be mapped to ANY device type
IoT/Device Testing Frameworks

Based on best practices, expert recommendations, and trusted industry guidance and standards:

- OWASP
- FTC Guidance
- FDA Guidance
- NIST
- IHE PCD
- ICSA Labs
Consumer Confidence is a Key to Adoption

In a Rapidly Evolving Environment Consumer Confidence is Key

• Certification provides independent third party assurance that software and devices can meet baseline requirements for functionality, interoperability, privacy, and security. Certification is not a panacea – however requiring certified products should be an important part of any defense-in-depth risk-based information security policy, as well as procurement policies.

• As reported by the FTC, a lack of consumer confidence that IoT and medical devices are safe, reliable, and secure will hinder adoption.

• The security landscape with regards to connected devices is akin to the Wild West – in order to ensure that the technology deployed tomorrow will deliver on the promises made today, the industry needs to double down on efforts to ensure products are built securely by design and follow key recommendations with regards to information governance.
Certification Can Drive Innovation

Certification Can Drive Product Developers to Compete Above the Bar

- **Ease the Barrier to Entry** – every day there are new Health IT devices and applications being churned out by entrepreneurs. Healthcare is one of the most exciting, lucrative, and potentially rewarding industries—but at the same time products and manufacturers are subject to a dizzying array of requirements and regulation. There’s no need to start from scratch or recreate the wheel - Certification spells out fundamental requirements by establishing a baseline of standards from which to begin development.

- **Going beyond minimum requirements** – Product development teams are not able to innovate if there is no demand for their product. Innovation does not occur by focusing only on minimum requirements. Certification requirements focus on industry vetted, mature standards, and a community of experts that can help developers save valuable time and resources to focus efforts on breaking new ground, improving workflow and usability, and delivering applications that meet or exceed user expectations.
Forging Ahead Despite Regulatory Uncertainty

Private-public Collaboration

• Programs like ConCert by HIMSS certification provide a contrast to government mandated programs by moving at the speed of the private sector, as opposed to the regulatory process – which cannot keep up with the pace of technology and innovation.

• ConCert engages the very stakeholders that design and use these technologies in order to develop certification and conformance requirements that more closely align with the “real world.” The focus remains on products that are available in the market and have the interoperability and security capabilities required for secure and reliable data exchange.

• Our current political landscape is projecting uncertainty as far as how regulations and regulatory agencies will take shape in the next year and beyond. Whether requirements are mandated, or not – cyber security is a pressing issue that cannot be delayed – the ConCert program will continue to engage the industry to further secure the healthcare environment.
ConCert by HIMSS™ Certification

Industry leaders collaborating to deliver production ready, secure, and interoperable Electronic Health Records (EHRs), Health Information Exchanges (HIEs), Health Information Service Providers (HISP), and Medical Devices.
Questions

Amit Trivedi
Program Manager, Healthcare
ICSA Labs
www.icsalabs.com | @a3vedi

Reminder: Please complete an online session evaluation!