

Cisco Medical Data Exchange Solution Technical Overview

Introduction

This document provides an overview of the Cisco Medical Data Exchange Solution (MDES), the industry drivers for the solution, and the solution architecture, components, and recommended configurations. The intended use for this document is to provide a sufficient understanding of the solution to enable positioning with a client. It is not a detailed implementation or design guide.

Overview

In today's modern healthcare environments, patients often receive medical treatment from a number of physicians, at different sites, based on any number of factors. To provide the optimum treatment for the patient, physicians require access to their patients' records as part of the overall care process. The records are typically fragmented within different healthcare organizations or, in many cases, restricted for use within a single healthcare system.

Optimum patient care requires that the records needed are shared between different healthcare providers. At present, the typical way to transfer the patient record is to either send a fax, make hard copies or, in the case of images, use electronic media such as a CD or DVD. To provide a complete picture of the patient's medical history, this process must be repeated by each physician who provided the patient with care. Alternatively, the data exchange becomes the responsibility of the patient to obtain copies and transport them between organizations.

This manual process is obviously expensive and inefficient for both the patient and physicians. In many cases, if a person needs to visit an emergency room in a location away from their primary healthcare provider, the records are simply not available. If the records are stored electronically, they probably conform to one or more electronic standards. Because there are various versions of those standards, consistency across vendors varies greatly. Even if the systems are interconnected, there is a good chance that the medical records on one system cannot be read on another.

As an example of the lack of interoperability that Cisco MDES can address, a leading healthcare provider in Europe struggled with providing a patient-centric view of data across its environment. This 1300 bed healthcare organization services an area comprised of 600,000 residents offering 24-hour specialized medical treatment. Prior to Cisco MDES, medical records consisted of disjointed paper copies of



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2011 Cisco Systems, Inc. All rights reserved.

medical records, segmented by facility. Where there were digital systems employed, incompatibility between the systems limited sharing among providers. The scope of the problem was widespread and involved 64 different systems using 1500 proprietary data interfaces, each with a different patient index. As a result, clinical documentation was rarely reused and it was difficult to integrate local physicians into the hospital environment. This organization suffered from degradation in care as well as high operational costs. This problem is not isolated to this specific healthcare system and exists globally in many healthcare organizations.

The Cisco MDES solution addresses these challenges and provides the means to create an intelligent infrastructure providing a patient-centric view of clinical information. It enables the network infrastructure to eliminate the operational costs of manual transport or proprietary health information exchanges (HIE) and reduce the delays associated with alternative solutions. The Cisco MDES solution integrates Integrating the Healthcare Enterprise (IHE[®]) standards-based applications from Tiani-Spirit onto a Cisco Unified Computing System Express (UCS Express) to form the basis for the efficient exchange of clinical information between disparate systems.

Integrating the Healthcare Enterprise (IHE)

IHE is a global non-profit organization that has developed a framework of standards that allows disparate systems to exchange medical data. The IHE defines *integration profiles* within various domains. Profiles consist of *actors* that perform certain roles, *transactions* that may be performed between these actors, and the formats and protocols used to execute transactions. There are nine defined domains including radiology, cardiology, pathology, and IT infrastructure. Within the IT infrastructure domain, there are twelve profiles, including Cross-Enterprise Document Sharing (XDS) and Patient Identifier Cross Referencing (PIX). Profiles use existing information standards such as HL7, CCOW, ebXML, CDA, and PDF for document formats and to execute these transactions. Cisco MDES complies with 79 IHE stars (actor/profile tests) based on the most recent North American IHE Connectathon 2011 testing. Specific information on the profiles the MDES supports and additional information on IHE is available at <http://www.ihe.net>. IHE Connectathon results are available at http://sumo.irisa.fr/con_result/.

The IHE framework uses the concept of *affinity domains*, which consist of a well-defined set of document registries/repositories and document sources/consumers that have agreed to share clinical documents. An affinity domain can be as small as a single provider organization or hospital, or can be much larger. In the logical data structure shown in [Figure 2](#), an affinity domain would be a Regional (orange) node and the local (yellow) nodes associated with that Regional node. This allows for a very small-scale implementation (one or two hospitals or groups) to implement the solution. As multiple instances of affinity domains are implemented over time, their simplified interconnection allows the healthcare providers to easily share their clinical information. This allows the system to grow from a few organizations to a larger regional, national, and international scale, avoiding the huge up-front investment of implementing from the top down with no guarantee of success.

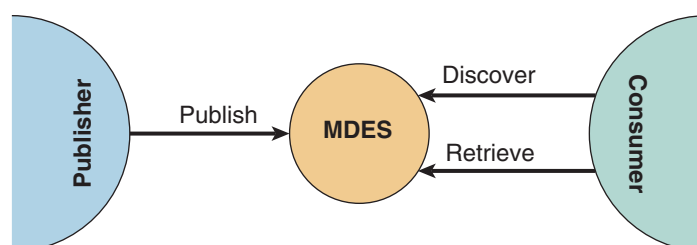
Even though disparate systems may comply with the different healthcare standards, they still may not be able to directly communicate. For example, different electronic health record (EHR) systems may implement different versions of HL7 (2.5 vs. 3.0). Cisco MDES is able to bridge the syntactic gaps that exist through its advanced transformation services.

There are two approaches to providing ubiquitous access to medical records. One is to create a central clinical data store. In this approach, all the medical information is uploaded to a central location. As the data is transferred to the central site, everything is converted to a vendor-independent format. The result is rapid, easy access to standardized records with redundancy and simplified backup. This approach, however, requires a very large central store to contain all the medical information, and therefore does not scale well. Although this approach may work well at the local and possibly regional level, it does not scale for larger deployments.

The second approach is to leave the medical data distributed at the local level and provide a means of indexing the patients and matching them with their records. This federated approach is extremely scalable because the only data that needs to be distributed through the network is the indexing data, which is very small. Because access to large files is usually confined to the local system, bandwidth typically is not an issue. This is the approach taken by the Cisco MDES solution.

Cisco MDES incorporates a master patient index and translation function directly into the network infrastructure. Patient records remain where they were created, but are accessible from anywhere within the healthcare network. The Tiani-Spirit IHE application runs on a Cisco SRE module located within a Cisco 3900 or 2951 Series Integrated Services Router (ISR). The patient index creates a registry of patients shared across the data exchange environment. Entities within this environment may be either consumers or publishers of information. [Figure 1](#) shows the basic functions provided to a publisher and consumer. A publisher needs an MDES instance (Cisco UCS Express) at its site. A consumer that does not publish information may not need an MDES instance, depending on the capabilities of the local application. There are several ways to integrate with systems to make participation in the exchange easier.

Figure 1 Solution Overview



Publish, Discover, Retrieve:

- Publisher
 - Exchange of test results and reports (lab, cardiology, radiology, imaging, medical summaries) community physician
 - Simple interface to the network, publishing made easy
- Consumer
 - Seamless, secure access to complete clinical information

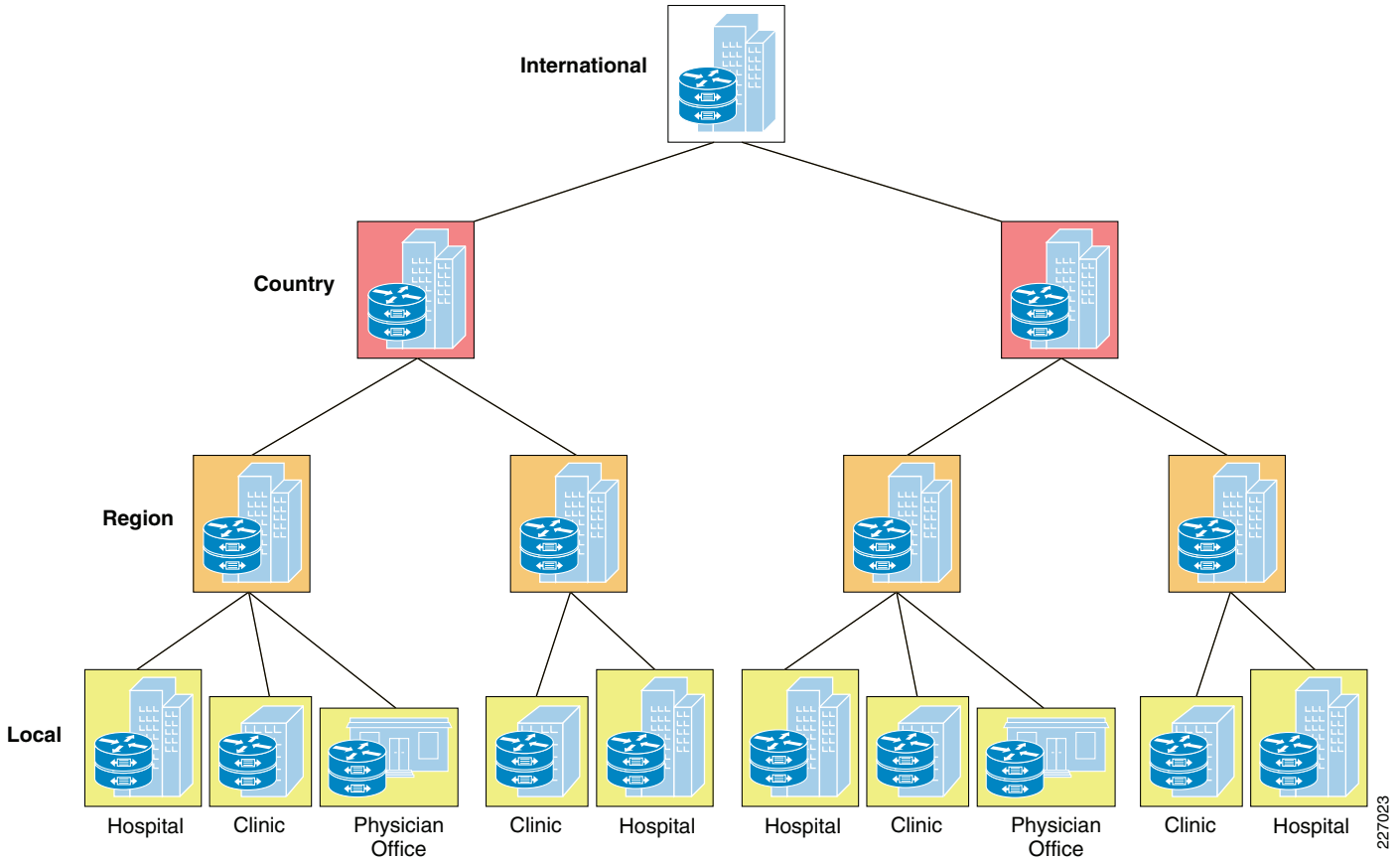
227022

The system is deployed in a federated structure, as shown in [Figure 2](#). The Cisco MDES solution communicates with the local record repositories (for example, CIS Healthcare and other IHE-compliant healthcare systems) and extracts patient indexing information. The information collected is then stored in a database residing on the SRE module. The patient index that was created is replicated one level higher in the hierarchical model to provide for high availability and redundancy. As long as the patient stays within his local system, the indexing data is never replicated beyond these two systems. In the event that the patient visits a remote facility outside their local healthcare system, the remote (requesting) system securely locates the patient's local healthcare system and provides the remote physician with a comprehensive list of the information that exists for the patient. An authorized care provider can access the records that their access rights allow, keeping the entire transaction in compliance with local privacy laws.

Any data translations that need to occur are performed by the network infrastructure and do not require additional software or customization to the clinical information systems involved in the information sharing transaction.

The new medical information gathered by the treatment of the patient at the remote site resides at the remote site. This information is now visible to the patient's local physician as those EMR systems are made aware of the new medical information. This meets the overall goal of achieving a seamless, patient-centric view of a patient's records and access to those records no matter where they are located.

Figure 2 Federated Data Structure Enabled by MDES (Logical View)



Solution Components

The Cisco MDES solution consists of the Tiani Spirit application running on an Cisco Unified Computing System (UCS) or Cisco Unified Computing System Express (UCS Express). Cisco UCS is a range of rack and blade servers, and Cisco UCS Express is a Services Ready Engine (SRE) running in a Cisco 3900 or Cisco 2951 Series Integrated Services Router (ISR). To achieve a federated design, these are distributed throughout the healthcare system based on data interoperability, publishing, and consuming factors. The particular platform deployed depends on the location in the network and the scale of the deployment.

Tiani Spirit

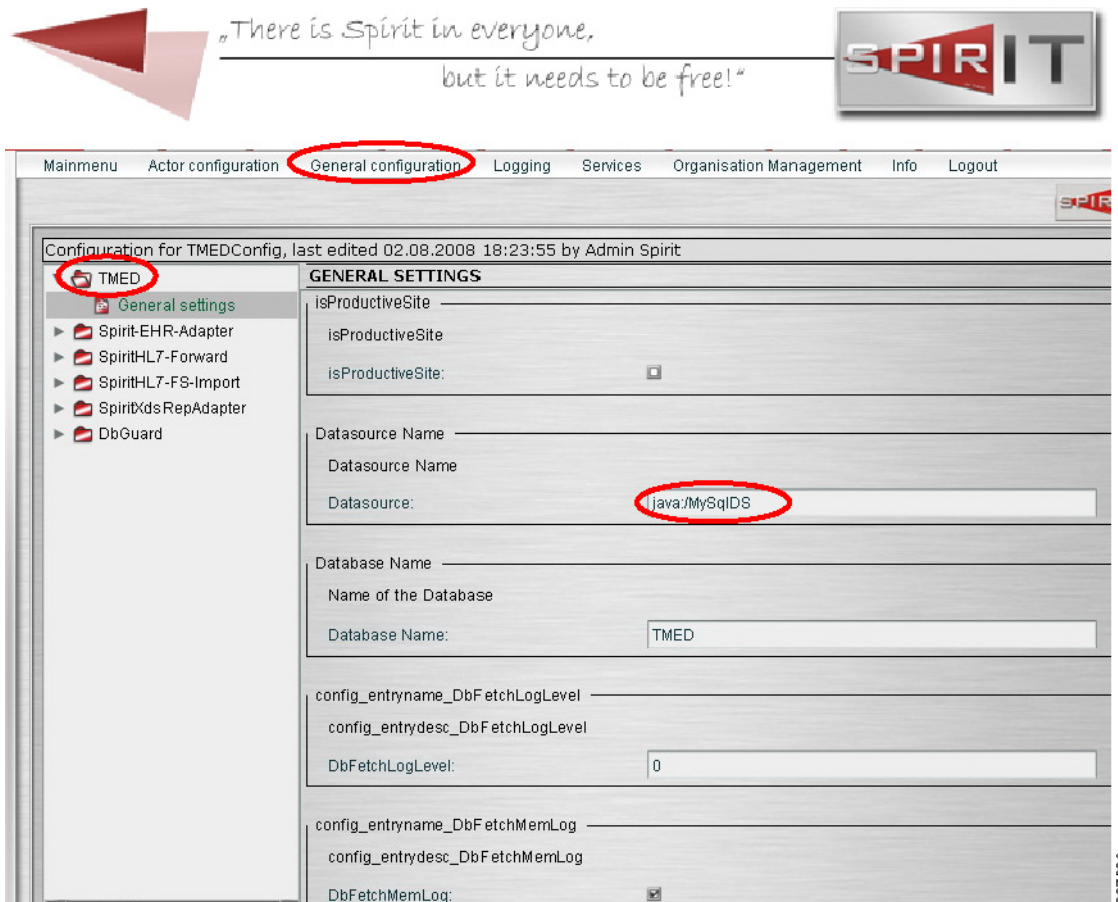
The Tiani Spirit application provides the middleware, patient indexing, and registry and compliance components to build a clinical information exchange. Running on Cisco USC or Cisco UCS Express, the application uses only the required functions as needed based on the operational demands and configuration.

The Tiani Spirit application is completely based on the IHE profiles. A graphical user interface based on Flash is provided for the configuration and monitoring of the application, as seen in [Figure 3](#) and [Figure 4](#).

Figure 3 Tiani-Spirit Web Admin Interface Login



Figure 4 Tiani-Spirit Web Admin Interface



The application provides adapters to allow the connection of legacy systems, such as hospital information systems, that are not IHE compliant but comply with standards such as HL7. The adapters provide functionality for protocol conversion and implement various IHE actors and the business logic required to connect into an IHE-based interoperable environment.

In normal operation, if the client is using client software (such as an EHR or EMR), the software is transparent, retrieving the information from the supplying system and delivering to the client system, with the client system providing the display and user interface. In the event a client is not available, a web application is provided for client-side viewing. Figure 5 and Figure 6 are sample screen shots from the web application.

Figure 5 Available Patients Partial Screen

Table (1 - 5 of 5)

	Surname	First Name	Middle Name	Title	BirthName	Sex	Birth Date	Info	Domain	Street Address	City	Province
	Indiana	Jones				♂	1911-11-11	●●●	005.12290842769873			
	Sparrow	Jack	Heart			♂	1950-06-09	●●●	005.122546 2127783	Mainstreet 23	Somewhere	This State
	Spirit	Naomi	Headache			♀	1982-07-01	●●●	005.1225463226521,005.12254628817555	Single Street 57	ThatTown	NiceLand
	Walker	Johnny	Knee			♂	1975-03-31	●●●	005.12257031938977,005.12257037495071	Glenmorangie Ave. 23	Glenfiddich	Dimple State
	Kent	Clark				♂	1976-06-09	●●●		Batman Blvd 23	Metropolis	Metropolis

Legend:

- Patient is local
- Patient is not local
- Patient has documents
- Patient has no documents

227027

Figure 6 Documents Available for an Individual Patient Partial Screen

Document Selection:

- All Departments (8)
- GeneralMedicine (3)
- Radiology (3)
- Primary Healthcare (2)
- All Participants (8-0)
- Practitioner (3-3)
- Central Hospital (5-5)
- All Doc Classes (0-0)
- Images (2-2)
- Referral (2-3)
- Visit Summary (1-1)
- No Value Provided (1-1)
- Referral Summary (1-1)
- All Confidentiality Levels (3-0)
- Usual control (6-6)
- Normal (2-2)
- Status (8-0)
- approved (8-8)
- Index (5-8)
- noFolder (0-0)

Selected Documents:

Access	Type	Status	Submission Time	Type	Class	Title	Participant	Department
●	●	●	2008-11-03 15:18:12	Referral Summary	Referral Summary	MRI left knee	Central Hospital	Primary Healthcare (Prim
●	●	●	2008-11-03 15:18:10	Visit Summary	Visit Summary		Central Hospital	Primary Healthcare (Prim
●	●	●	2008-11-03 10:55:18	Diagnostic Imaging	Images	L KNEEPAIN	Central Hospital	Radiology (Radiology)
●	●	●	2008-11-03 10:55:12	No Value Provided	No Value Provided	Prescription	Practitioner	General Medicine (Gene
●	●	●	2008-11-03 10:53:06	Referral Request	Referral	Request MRI left knee	Practitioner	General Medicine (Gene
●	●	●	2008-11-03 10:31:08	Referral Summary	Referral	Radiology Report plain X-ray knees	Central Hospital	Radiology (Radiology)
●	●	●	2008-11-03 10:15:34	Diagnostic Imaging	Images	Left Knee an	Central Hospital	Radiology (Radiology)
●	●	●	2008-11-03 10:07:56	Referral Request	Referral	Request plain X-Ray both knees ap anc	Practitioner	General Medicine (Gene

227028

The web application provides client-side functionality for the following:

- Patient management
- Document management
- Patient duplicate management
- Access to the audit record repository
- Access to the internal logging

For more information on Tiani Spirit, see <http://www.tiani-spirit.com>.

Cisco Services Ready Engine

Cisco Services Ready Engine (SRE) modules are router blades for the second generation of Cisco ISR G2s that provide the capability to host Cisco, third-party, and custom applications. SRE modules come in internal service module (ISM) and service module (SM) form factors. Cisco MDES is not supported on the ISM model. [Table 1](#) lists the features of the supported SRE modules.

Table 1 *Features of Supported SRE Modules*

Feature	Cisco SRE 710 SM	Cisco SRE 910 SM
Form factor	Service module (SM)	Service module (SM)
CPU	Intel Core 2 Solo 1.86 GHz	Intel Core 2 Duo 1.86 GHz
DRAM	4 GB	4–8 GB
Compact Flash memory	2-GB internal USB flash-memory module	2-GB internal USB flash-memory module
Hard disk	One 500 GB	Two 500 GB (1 TB in non-redundant array of independent disks (RAID) mode)

SRE modules provide the compute platform onsite in hospitals, clinics, and large physician practices. The router platform hosting the SRE also provides routing/switching, security, and unified communications services.

The platform supported for the onsite systems is the Cisco UCS Express, which comprises the following:

- Cisco SRE multipurpose x86 blade servers
- Cisco SRE virtualization powered by VMware vSphere Hypervisor (currently ESXi 4.1)
- Cisco Integrated Services Routers Generation 2 (ISR G2) with Multigigabit Fabric (MGF) backplane switch
- Cisco Integrated Management Controller Express (CIMC Express)

[Figure 7](#) shows the Cisco ISR Generation 2 and SRE.

Figure 7 Cisco Integrated Services Routers Generation 2 and Services Ready Engines



This is typically deployed with two SRE modules; one running the application and web server, and the second hosting LDAP and the database application. In light use environments, the solution may be deployed with a single SRE.

For more information on Cisco SREs and Cisco UCS Express, see <http://www.cisco.com/go/ucse>.

Cisco Unified Computing Platform

The Cisco UCS integrates a low-latency unified network fabric with enterprise-class, x86- architecture servers along with virtualization resources (see [Figure 8](#)). The system is an integrated, scalable, modular platform in which all resources participate in a unified management domain. A single system scales to up to 40 blade chassis, 320 compute nodes, and thousands of virtual machines.

Figure 8 Cisco B Series Unified Computing Systems



Cisco UCS C-Series Rack-Mount Servers extend the Cisco UCS to a rack-mount form factor, including a standards-based unified network fabric, Cisco VN-Link virtualization support, and Cisco Extended Memory Technology. (See [Figure 9](#).)

Figure 9 Cisco C Series Unified Computing Systems



Cisco UCS B- and C-Series servers provide the MDES compute platform when the SRE-based solutions do not provide sufficient scale, and in locations where the UCS platforms are already deployed. In the UCS environment, the MDES components are deployed as virtual machine instances. This testing uses VMware's vSphere Enterprise 4.1, which allows easy migration of virtual machines between the compute platforms.

For more information on the Cisco Unified Computing System, see <http://www.cisco.com/go/ucs>.

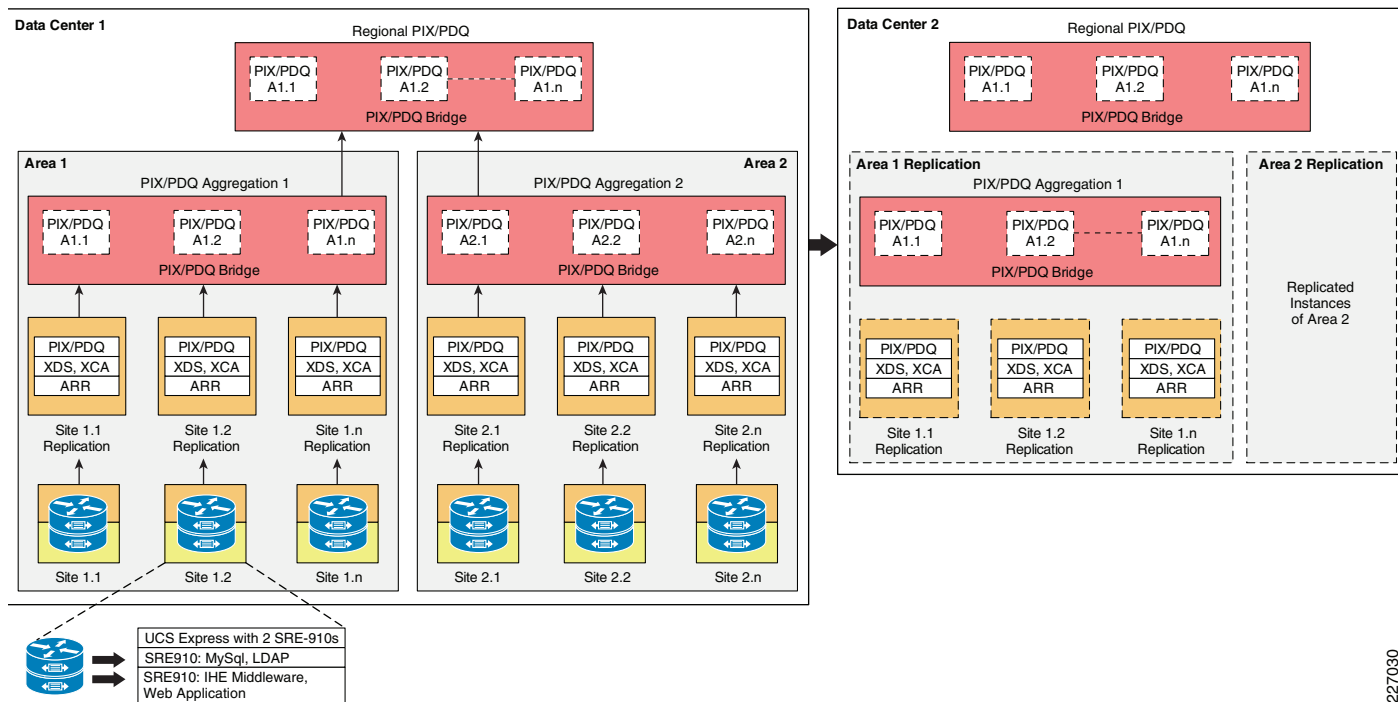
Solution Architecture

This solution is deployed in a federated fashion as shown in Figure 2. At the local level, a Cisco UCS Express with one or more SRE modules is located at a hospital or clinic, or shared between individual physicians and/or smaller clinics. At the regional level, either a UCS Express with one or more SRE modules is deployed for each remote node or (more likely), a UCS is deployed with virtual machines for each remote node. At the national level, a UCS is used to aggregate a number of regional nodes.

Systems that are IHE compliant may possibly communicate directly to higher-level nodes in the IHE federation. Legacy systems that are non-IHE compliant but support standards such as HL7 require an MDES node to run an adapter to convert the standard messages into IHE-compliant messages with the appropriate IHE business logic.

Figure 10 is representative of a global architecture from a typical deployment.

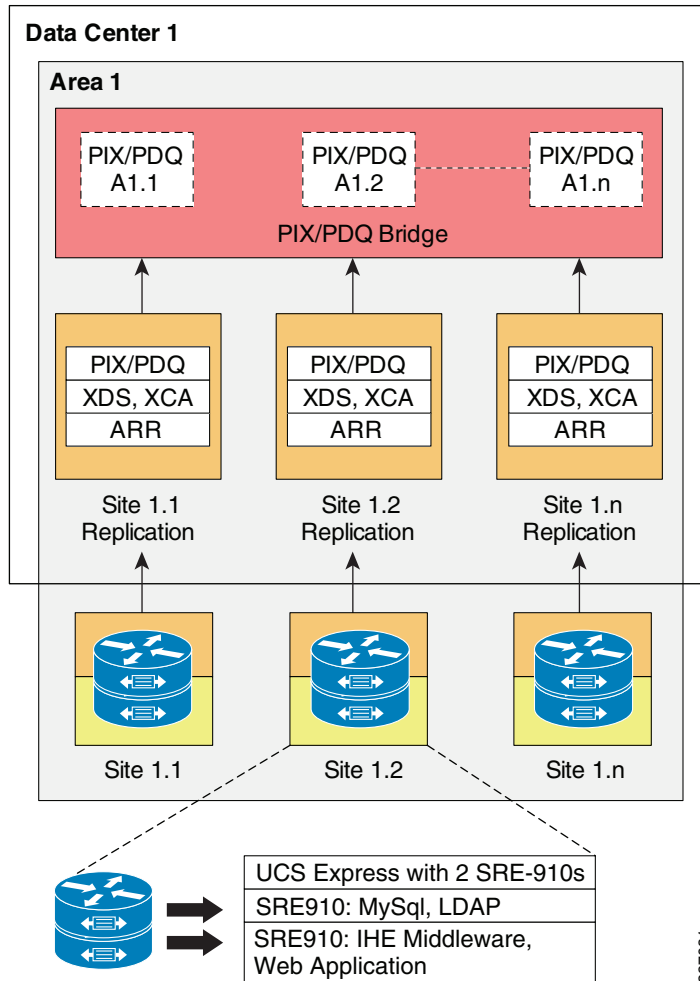
Figure 10 MDES Deployment Hierarchy (System View)



For the edge node, a Cisco ISR 2951 or 3925 with a pair of SRE-910 modules is recommended. In this configuration, the SQL database and LDAP-based user database run on one SRE module, and web services, along with the Spirit application, run on the second SRE module, as shown in Figure 11.

227030

Figure 11 IHE Autonomous System



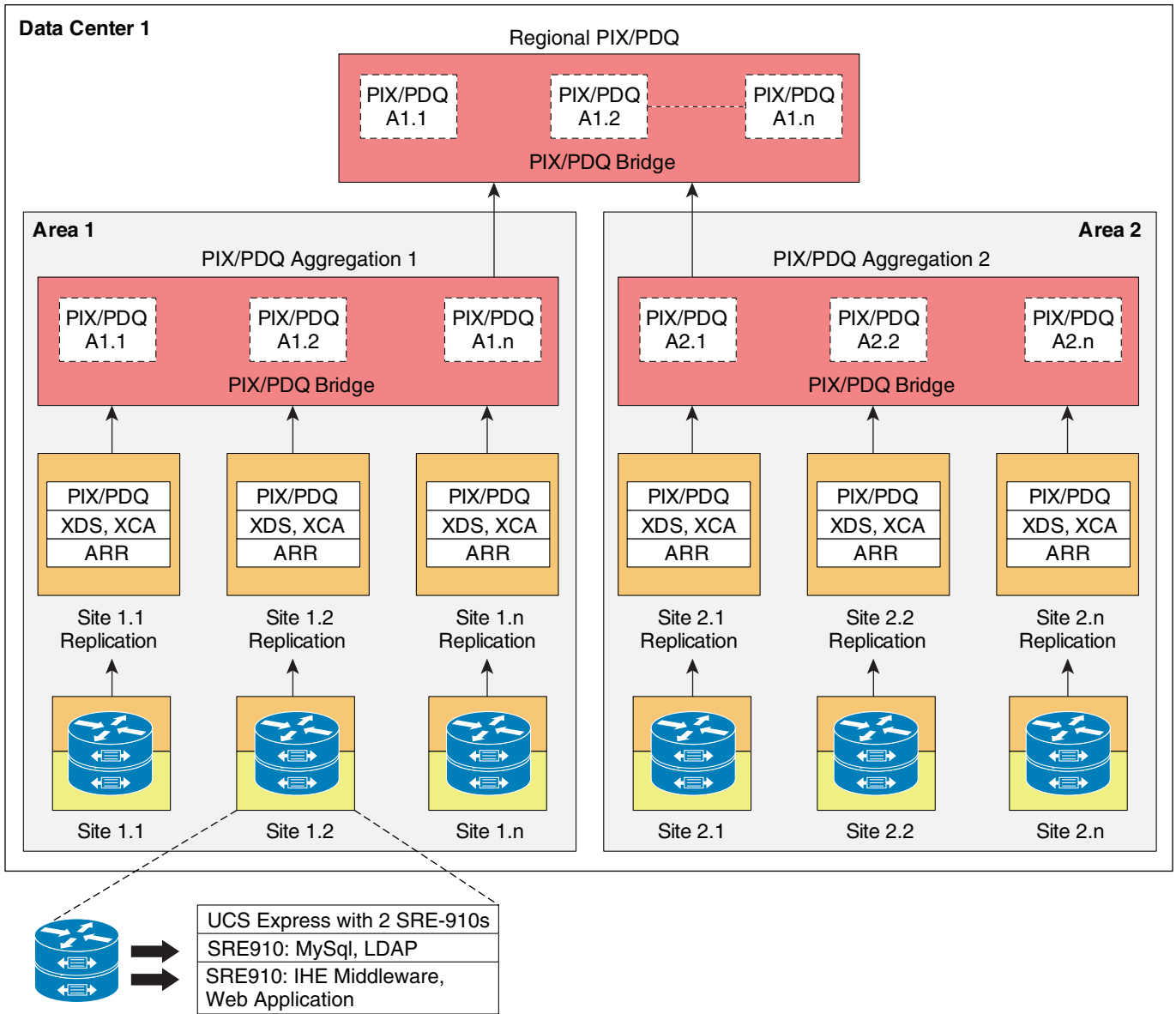
This configuration can handle up to 100,000 patients/exams per year and between 25 and 50 concurrent users. This is sufficient for a medium-sized clinic. Larger facilities will of course exceed this capacity and require an additional ISR 3925 for each 100,000 patients/exams. For a site running bandwidth intense application (such as an Oncology Center), the same approach is used but should be scaled at each 50,000 patients/exams per year.

In this configuration, the Orange layer is extended into the facility. This allows the facility to operate autonomously in the event of network issues and provides maximum reliability.

The information in the facility is replicated in the next layer up. In Figure 11, this is in Data Center 1. For additional reliability the data should also be replicated in a second data center (see Figure 10). For each edge node, an ISR 3945 with four SRE-910 modules is required in one of the two data centers. This provides for both a primary and backup copy of the remote SRE. The primary image for a site is stored on two SRE modules in an ISR in Data Center 1 and the backup on a second pair of SRE modules in Data Center 2, or as a VM on a UCS in Data Center 1 and a backup VM on a UCS in Data Center 2.

The red blocks may also be run on Cisco UCS Express, depending on the match and link location. In Figure 12, match and link are performed in the Regional red block and the lower level red nodes are just notified.

Figure 12 Cross-Domain Indexing



227032

A router is sufficient to do the match and link function for up to 1 million patients. For clinical repositories serving more than 1 million people, a Cisco Unified Computing System is required.

Table 2 lists the hardware requirements.

Table 2 Hardware Requirements

Level	Router	SRE Model	Software Execution
Patient Index (Red)	CISCO3945	SRE-910	SRE1: DB, LDAP SRE2: Spirit SRE3: Backup of AXP1 SRE4: Backup of AXP2
Cross-Enterprise (Orange)	CISCO3945	SRE-910	SRE1: DB, LDAP for Enterprise Location 1 ¹ SRE2: Spirit, Web for Enterprise Location 1 ¹ SRE3: DB, LDAP for Enterprise Location 2 ¹ SRE4: Spirit, Web for Enterprise Location 2 ¹
Local (Yellow/Orange)	CISCO3925 CISCO2951	SRE-910	SRE1: DB, LDAP SRE2: Spirit, Web

1. Primary/Backup for each Enterprise location will be split across 2 Orange Level routers.

Security Considerations

In healthcare, patient privacy and security is always a primary concern. The Canadian Personal Information Protection and Electronic Documents Act (PIPEDA), the United States’ Health Insurance Portability and Accountability (HIPAA) Act, Europe’s EC 95/46 Directive, and Japan’s HPB 517 regulate the privacy of identifiable patient information. The Audit Trail and Node Authentication (ATNA) Integration Profile establishes security measures which, together with the Security Policy and Procedures, provide patient information confidentiality, data integrity, and user accountability. ATNA limits access between nodes and limits access to a node to authorized users. Network communications between secure nodes in a secure domain are restricted to only other secure nodes in that domain. Secure nodes limit access to authorized users as specified by the local authentication and access control policy. ATNA provides for an audit trail to allow security officers to insure compliance with a security domain’s policies. The MDES application implements both Secure Node (SN), Secure Application (SA), and the Audit Record Repository (ARR) actors. The MDES solution generates audit logs on each PHI access transaction it performs and forwards to the ARR. For further information, see <http://www.ihe.net>.

Appendix—Relevant IHE Actors Implemented in the Tiani Spirit Application

These IHE Actors (Profile) are implemented:

- Server-side Actors:
 - Patient Identifier Cross-referencing (PIX) Manager
 - Patient Demographics Query (PDQ) Supplier
 - Cross-Enterprise Document Sharing (XDS) Document Registry (XDS.a/b)
 - Cross-Enterprise Document Sharing (XDS) Document Repository (XDS.a/b)
 - Cross-Enterprise Document Sharing for Imaging (XDS-I) Imaging Document Source

- Personnel White Pages (PWP) Directory
- Audit Trail and Node Authentication (ATNA) Audit Record Repository
- Cross-Enterprise User Assertion (XUA) X-Service Provider
- Cross-Community Access (XCA) Initiating Gateway
- Cross-Community Access (XCA) Responding Gateway
- Client-side Actors:
 - Patient Identifier Cross-referencing (PIX) Consumer
 - Patient Demographics Query (PDQ) Consumer
 - Cross-Enterprise Document Sharing (XDS) Document Consumer (XDS.a/b)
 - Cross-Enterprise Document Sharing for Imaging (XDS-I) Imaging Document Consumer
 - Cross-Enterprise Document Sharing for Medical Summaries (XDS-MS) Content Consumer
 - Personnel White Pages (PWP) Consumer
 - Cross-Enterprise User Assertion (XUA) X-Service User
 - Basic Patient Privacy Consents (BPPC) Content Consumer
- Common/Bundled Actors:
 - Audit Trail and Node Authentication (ATNA) Secure Node
 - Audit Trail and Node Authentication (ATNA) Secure Application
 - Consistent Time (CT) Time Client

For More Information

- Solution manager—Doshi Hemanshu (hemdoshi@cisco.com; +65 6317 7679)
- Technical marketing engineer—Wen-Pai Lu (wenlu@cisco.com; +1 408 527 6557)
- SRE product manager—John Voss (jovoss@cisco.com; +1 408 421 1323)
- Tiani “Spirit”—<http://tiani-spirit.com>
 - Sales—Brett Crown (brett.crown@tiani-spirit.com; +1 301 473 1293)
 - Technical—Tony Anderson (tony.anderson@tiani-spirit.com; +1 678 576 1907)
- Tiani “Spirit” implementation partners—Xtension (<http://www.x-tention.at>)

