

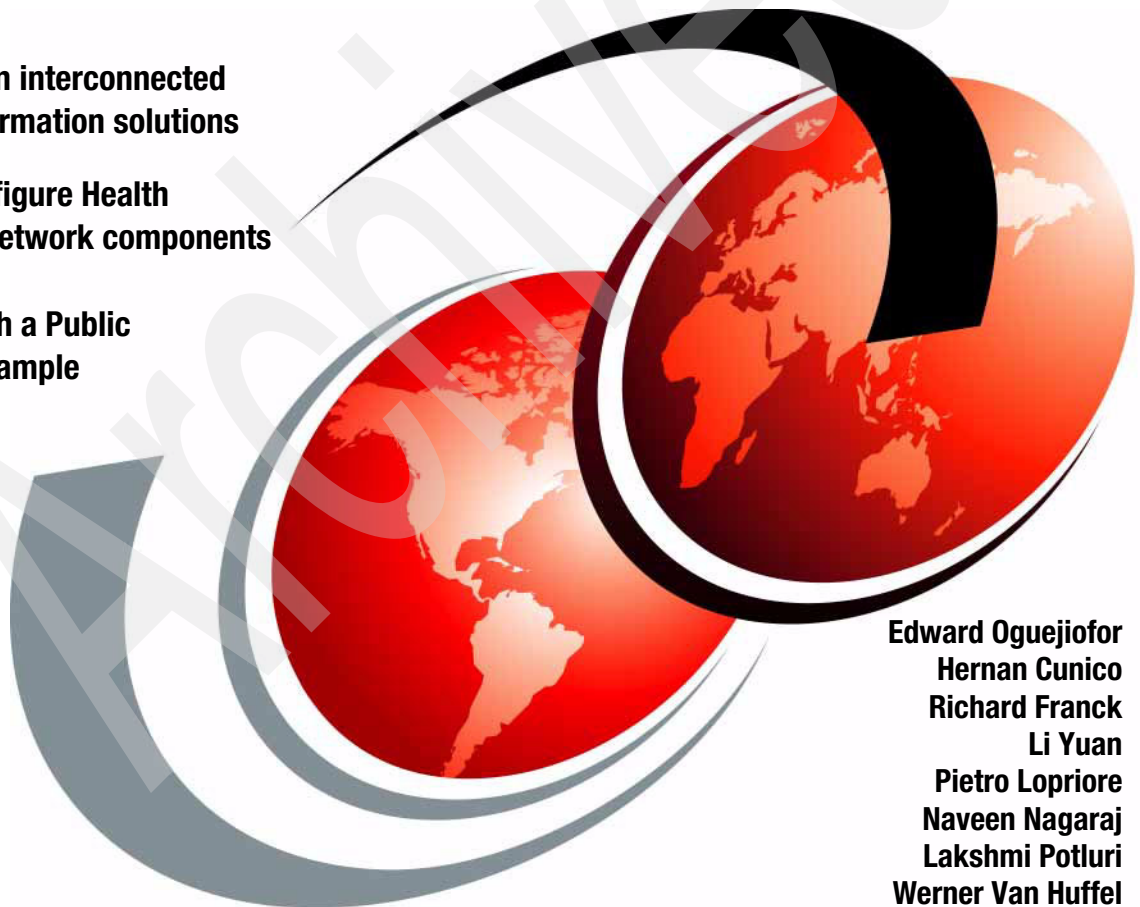
Healthcare Collaborative Network

Solution Planning and Implementation

Plan and design interconnected healthcare information solutions

Install and configure Health Collaborative Network components

Get started with a Public Health Alert example



Edward Oguejiofor
Hernan Cunico
Richard Franck
Li Yuan
Pietro Lopriore
Naveen Nagaraj
Lakshmi Potluri
Werner Van Huffel



International Technical Support Organization

**Healthcare Collaborative Network: Solution
Planning and Implementation**

February 2006

Archived

Note: Before using this information and the product it supports, read the information in “Notices” on page vii.

First Edition (February 2006)

This edition applies to Release 1.0 of WebSphere Business Integration for Healthcare Collaborative Network, product #5724-J12.

© Copyright International Business Machines Corporation 2006. All rights reserved.

Note to U.S. Government Users Restricted Rights -- Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

Notices	vii
Trademarks	viii
Preface	ix
The team that wrote this redbook	xi
Become a published author	xiii
Comments welcome	xiv
Chapter 1. Introduction to Healthcare Collaborative Network	1
1.1 Overview of Healthcare Collaborative Network	2
1.1.1 The origins of Healthcare Collaborative Network	3
1.1.2 Trends enabling Healthcare Collaborative Network	5
1.1.3 How Healthcare Collaborative Network works	6
1.1.4 Benefits of Healthcare Collaborative Network	11
1.2 Solution models	15
1.3 Public Health Alert scenario	17
1.3.1 The scenario	18
1.3.2 Organizations	20
1.3.3 Publishers	22
1.3.4 Subscribers	23
1.3.5 The topics	24
1.4 Chapter summary	25
Chapter 2. Planning and designing your HCN solution	27
2.1 Stages of the HCN solution	28
2.1.1 Preinstallation stage	29
2.1.2 Installing the HCN	36
2.1.3 Postinstallation	39
2.2 Solution sub-plans	42
2.2.1 Planning for education	42
2.2.2 Planning for software	45
2.2.3 Planning for hardware	49
2.2.4 Planning for networking	54
2.2.5 Planning for data interoperability	55
2.2.6 Planning for capacity and performance	57
2.2.7 Planning for privacy and security	58
2.2.8 Planning for service and support	60
2.3 Chapter summary	61

Chapter 3. Installing and configuring IBM WebSphere Business Integration for HCN	63
3.1 Solution installation overview	64
3.2 Installation requirements and prerequisites	64
3.2.1 Hardware requirements	65
3.2.2 Software prerequisites	66
3.3 Installing the Healthcare Collaborative Network hub	71
3.3.1 Message Flow server	71
3.3.2 Administrative server	72
3.3.3 AGPI server	73
3.4 Installing the Healthcare Collaborative Network gateway	74
3.4.1 Starting connector agents	77
3.5 Configuring HCN security features	79
3.6 Validating the installation	87
3.6.1 Validating the WebSphere MQ configuration	89
3.6.2 Validating HCN data flow	92
3.7 Chapter summary	96
Chapter 4. HCN entities and functional components	97
4.1 HCN entities and functional components overview	98
4.2 Organizations	99
4.3 Gateways	101
4.4 User roles	103
4.4.1 Administrator role	104
4.4.2 Observer role	114
4.4.3 Subscriber role	116
4.4.4 Publisher role	128
4.4.5 Publisher and Subscriber role	135
4.5 Privacy levels	135
4.6 Notifications and e-mails	136
4.7 Health topics	141
4.7.1 Quality of Care	142
4.7.2 Adverse Drug Events	143
4.7.3 Public Health Alerts	145
4.7.4 XML Only Content	145
4.8 Chapter summary	146
Chapter 5. System management	147
5.1 HCN Administrative and AGPI servers	148
5.1.1 Log files	148
5.1.2 LDAP administration	149
5.1.3 Administrative server hints and tips	150
5.2 Message Flow server	151

5.2.1 Log files	151
5.3 Gateway	151
5.3.1 Gateway log files	151
5.3.2 Running gateway components as Windows services	152
5.3.3 Gateway tracing	157
5.4 General system management issues	159
5.4.1 WebSphere MQ queues and Queue Managers	159
5.4.2 HCN application databases	162
5.4.3 Backup and recovery	162
5.5 Chapter summary	163
Chapter 6. Privacy and security	165
6.1 Introduction to privacy and security	166
6.2 Privacy in HCN	166
6.3 Security in HCN	171
6.4 Privacy and security in the Public Health Alert scenario	174
6.5 Chapter summary	180
Appendix A. Customizing Healthcare Collaborative Network	181
Preparing the HCN development environment	182
Creating additional connectors	187
Mapping local clinical codes	203
Modifying or extending the predefined codesets	207
Observations or lab codes	210
Customizing HCN privacy rules	211
Modifying existing privacy levels	212
Creating and deleting privacy levels	219
De-identifying XML messages	221
Consolidating HL7 messaging variation	222
Appendix B. Health Level 7 overview	225
Introduction to Health Level 7	226
HL7 message structure	228
Structural presentation of HL7 messages	230
Types of HL7 messages	231
Appendix C. Performance tuning	235
Publisher gateway performance	236
Polling	236
Gateway connector performance	240
HCN subscriber gateway performance	242
WebSphere Business Integration server performance	242
HCN Message Flow server performance	242
Database performance	242

Abbreviations and acronyms 243

Related publications 245

IBM Redbooks 245

Online resources 245

How to get IBM Redbooks 246

Help from IBM 246

Index 247

Archived

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing, IBM Corporation, North Castle Drive Armonk, NY 10504-1785 U.S.A.

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrates programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. You may copy, modify, and distribute these sample programs in any form without payment to IBM for the purposes of developing, using, marketing, or distributing application programs conforming to IBM's application programming interfaces.

Trademarks

The following terms are trademarks of the International Business Machines Corporation in the United States, other countries, or both:

@server®	DB2 Universal Database™	Redbooks™
@server®	DB2®	Tivoli®
Redbooks (logo)  ™	IBM®	WebSphere®
xSeries®	OS/2®	

The following terms are trademarks of other companies:

Java, JDBC, JVM, J2EE, and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

Microsoft, Windows, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Intel, Intel logo, Intel Inside logo, and Intel Centrino logo are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States, other countries, or both.

Other company, product, or service names may be trademarks or service marks of others.

Preface

The IBM® WebSphere® Business Integration for Healthcare Collaborative Network is a health information infrastructure for interconnecting and coordinating the delivery of information to participants in the collaborative network electronically. Data source organizations, such as hospitals, physicians, and clinics, generate and communicate clinical data to data review organizations, such as pharmaceutical companies and government healthcare agencies. Healthcare Collaborative Network provides a real-time, secure, and reliable electronic infrastructure for collaboration between the two types of organizations.

By enabling immediacy and the ability to securely disseminate clinical health data, Healthcare Collaborative Network solutions participants can respond rapidly to health risks such as adverse drug effects, to manage quality of care, and implement monitoring and warning system for detecting the onset of dangerous infectious diseases or bioterrorism attack. Healthcare Collaborative Network supports all this while improving operating efficiencies in these organizations.

If you are a solution architect or a consultant or if you have the responsibility to create an interoperable health information infrastructure, then this IBM Redbook is aimed at you. It provides a first-hand guide for creating solutions based on the IBM WebSphere Business Integration for Healthcare Collaborative Network.

This redbook includes an example of a public health alert scenario. Although simple in nature, this working example demonstrates how you can use Healthcare Collaborative Network to manage pandemic preparedness and response. Throughout the book, we reference this scenario and present approaches for creating general solutions based on Healthcare Collaborative Network.

This book includes the following chapters:

- ▶ Chapter 1, “Introduction to Healthcare Collaborative Network” on page 1 provides an overview of the Healthcare Collaborative Network solution, discusses solution models, and describes the public health alert example solution scenario.
- ▶ Chapter 2, “Planning and designing your HCN solution” on page 27 describes the three stages of Healthcare Collaborative Network solution and discusses the considerations at each stage to enable you to create a project plan that is unique for your Healthcare Collaborative Network solution.
- ▶ Chapter 3, “Installing and configuring IBM WebSphere Business Integration for HCN” on page 63 provides installation and configuration guidelines. It also describes hints, tips, and lessons learned from installing Healthcare Collaborative Network solutions in our test environment.
- ▶ Chapter 4, “HCN entities and functional components” on page 97 enumerates the different user roles that are defined in Healthcare Collaborative Network and describes the different tasks that each user role can perform and the services that are available to the user.
- ▶ Chapter 5, “System management” on page 147 provides an overview of the different aspects of the key components of Healthcare Collaborative Network that you can administer and control.
- ▶ Chapter 6, “Privacy and security” on page 165 describes the privacy and security features supported in Healthcare Collaborative Network. This chapter also describes how security and privacy is implemented in the working example.
- ▶ The appendixes describe the features of Healthcare Collaborative Network that you can customize, introduce HL7, and discuss how to tune your Healthcare Collaborative Network solution to ensure that the performance is optimal.

The team that wrote this redbook

This redbook was produced by a team of specialists from around the world working at the International Technical Support Organization (ITSO), Raleigh Center.



The IBM redbook team, left to right: Werner Van Huffel, Pietro Lopriore, Naveen Nagaraj, Li Yuan, Richard Franck, Lakshmi Potluri, Edward Oguejiofor, and Hernan Cunico

Edward Oguejiofor is a project leader at the ITSO, Raleigh Center. He has over 20 years experience in distributed and enterprise systems architecture, design, and consulting. His areas of expertise include Web Services and Service Oriented Architecture. He also provides technical and thought leadership in emerging technologies and collaborative services. He holds a degree in Computer Science from Imperial College of Science and Technology.

Hernan Cunico is a Certified Consulting IT Specialist and WebSphere software specialist at the ITSO, Raleigh Center. He writes extensively and teaches IBM classes on WebSphere software. Hernan has 12 years of experience in the Information Technology and e-business consulting areas. His areas of expertise also include networking, security, e-business and e-commerce solutions architecture design and implementation.

Richard Franck is an IT architect in IBM Software Group, Public Sector Solutions, based in Research Triangle Park, North Carolina. He has 16 years of experience in IBM as a software developer, software development manager, and IT architect. He holds a BS in Computer Science and Psychology from Iowa State University. His work in the healthcare field has focused on cross-enterprise collaboration, clinical integration, and healthcare terminology.

Li Yuan is a Software Engineer in the On Demand Solution Center based in IBM China Development Lab. He has five years of experience in the enterprise application integration, content management and enterprise collaboration fields. Now he is primarily focusing on healthcare solution architect design and implementation. He holds a degree in Computer Science from Tong Ji University. His areas of expertise and interest include healthcare business integration, pandemic disease preparedness and biosurveillance, and electronic health records.

Pietro Lopriore is a Healthcare and Life Sciences Technical Sales Specialist in IBM Italy. He has six years of experience in architectural design, consulting and application development for Healthcare, Life Sciences and Banking companies. He holds a degree in Chemical Engineering from the Politecnico di Torino, Italy. His areas of expertise include bioinformatics, enterprise content management, regulatory compliance and on demand integration technologies. He has written about pharmaceutical and healthcare process management.

Naveen Nagaraj is a Staff Software Engineer at the IBM India Software Lab, Bangalore. He has worked at IBM for five years. He has experience supporting, debugging and testing Public sector industry solutions focused on the healthcare industry. Other experiences include supporting IBM Middleware products, and testing OS/2® Kernel and Networking. Naveen holds a Bachelors degree in Electronics and Communication.

Lakshmi Potluri has experience architecting, implementing, and integrating IBM Middleware technologies for various public sector industry solutions with special focus on the healthcare industry solutions. She has experience working on business development activities and technical training in Europe and Latin America . Lakshmi holds a Bachelors degree in Mathematics and a Master of Science in Computer Science. She has more than 14 patents pending in various areas of technology, has written several papers and has presented at prestigious internal IBM and external conferences.

Werner Van Huffel is a WebSphere Business Integration Technical Specialist, specializing in Healthcare Integration for the Australia and New Zealand region. He has over 10 years of experience in the integration field and over 20 years in healthcare IT. He holds a degree in Mathematics and Computing Science from the University of New South Wales, Australia, and is finalizing a Masters degree in Health Sciences (Health Informatics) from the University of Sydney, Australia. His areas of expertise and interest include enterprise business integration, electronic health records, healthcare security and privacy, healthcare change management and healthcare messaging.

Thanks to the following people for their contributions to this project:

IBM Pacific Development Center, Burnaby, BC, Canada

- ▶ Bryce Jeannotte
- ▶ Freddy Echeverri

IBM Software Group

- ▶ David Dean

IBM Corporate Headquarters, Governmental Affairs

- ▶ Ned McCulloch

Thanks to the following people from the ITSO, Raleigh Center

- ▶ Margaret Ticknor
- ▶ Tamikia Barrow
- ▶ Jeanne Tucker

Become a published author

Join us for a two- to six-week residency program! Help write an IBM Redbook dealing with specific products or solutions, while getting hands-on experience with leading-edge technologies. You'll team with IBM technical professionals, Business Partners, or customers.

Your efforts will help increase product acceptance and customer satisfaction. As a bonus, you'll develop a network of contacts in IBM development labs, and increase your productivity and marketability.

Find out more about the residency program, browse the residency index, and apply online at:

ibm.com/redbooks/residencies.html

Comments welcome

Your comments are important to us!

We want our Redbooks™ to be as helpful as possible. Send us your comments about this or other Redbooks in one of the following ways:

- ▶ Use the online **Contact us** review redbook form found at:

ibm.com/redbooks

- ▶ Send your comments in an e-mail to:

redbook@us.ibm.com

- ▶ Mail your comments to:

IBM Corporation, International Technical Support Organization
Dept. HZ8 Building 662
P.O. Box 12195
Research Triangle Park, NC 27709-2195

Introduction to Healthcare Collaborative Network

This chapter introduces the IBM WebSphere Business Integration for Healthcare Collaborative Network (HCN). It provides an overview of HCN. It then describes the key components and shows how you can leverage the HCN infrastructure to create solutions. This chapter also introduces solution models and concludes the chapter by describing a public health alert scenario that we use throughout the remainder of this book as a working example to show how you can use HCN to create a solution.

This chapter includes the following sections:

- ▶ Overview of Healthcare Collaborative Network
- ▶ Solution models
- ▶ Public Health Alert scenario
- ▶ Chapter summary

1.1 Overview of Healthcare Collaborative Network

IBM WebSphere Business Integration for HCN enables the exchange of healthcare messages and documents between and within organizations. In short, HCN enables electronic collaboration among entities who currently exchange data by less reliable or less timely means, or among entities who wish to establish the exchange of clinical healthcare information.

The reasons for exchanging data are many and varied, including:

- ▶ Making informed patient care decisions
- ▶ Monitoring quality of care (conformance to recommended treatment protocols)
- ▶ Determining if treatments were necessary and reasonable for the purposes of making payments for those treatments
- ▶ Responding to healthcare emergencies such as bioterrorism and public health threats
- ▶ Performing studies of population health
- ▶ Conducting research into the effectiveness of existing and emerging treatment protocols, drugs, and medical devices
- ▶ Conducting research into the intersection between a person's genetic makeup and their health

Timely communication and speed of response are vital for supporting the healthcare continuum of prevention, diagnosis, treatment and recovery. In cases of bioterrorism or disease outbreak, speed of response is crucial for the prevention of further exposure and infection.

An equally varied list of organizations and individuals collaborate in a network for sharing clinical information, including:

- ▶ Healthcare providers (hospitals, clinics, physicians, public health providers, specialists)
- ▶ Independent laboratories
- ▶ Community pharmacies
- ▶ Public health agencies (local, regional and national)
- ▶ Pharmaceutical and medical device manufacturers
- ▶ Researchers (academic, government, and independent)
- ▶ Payers (government or private insurers)
- ▶ Patients

Participants typically form healthcare ecosystems at community, regional, national and global levels. The picture today is that of the participants operating in information silos. Already fragmented, these ecosystems are being subjected to evolutionary forces. The recent outbreak of Severe Acute Respiratory Syndrome (SARS) is an example where the emergence of infectious disease quickly became a healthcare emergency on a global scale as a result of the ease of global travel. The potential for global epidemics coupled with the current heightened state of alert for possible bioterrorism attacks creates an urgent need to put in place early detection and quick response systems that integrate these various healthcare ecosystems.

Information technology is central to the realization of public health infrastructure that will integrate the healthcare ecosystems and enable the sharing of key clinical data across disparate applications and systems. IBM tapped its extensive business and technology expertise in the healthcare industry to create the IBM Aligned Clinical Environment. The Aligned Clinical Environment combines business insights, tools and methodologies to create an information technology on-demand environment for addressing critical needs of the healthcare industry such as cohabitation within healthcare ecosystems.

IBM has developed HCN for interconnecting and coordinating the delivery of information to participants in healthcare ecosystems. HCN relies on the information technology infrastructure and methodologies of the Aligned Clinical Environment to realize the solution.

In the sections that follow, we introduce HCN starting with a look at the origins of HCN and the trends that have made HCN a necessity in the healthcare industry. We also present an overview of how HCN works and conclude by discussing some of the benefits of HCN.

1.1.1 The origins of Healthcare Collaborative Network

The initial concept for HCN came from The eHealth Initiative and Connecting for Health, two organizations whose missions include driving improvement in the quality of care and safety, and efficiency of healthcare through use of clinical data and information technology. The initiative brought together healthcare industry leaders and leading technology providers. IBM contributed project management support, technical design, development and subject matter expertise.

The HCN initiative implemented a proof-of-concept project, the goal of which was to demonstrate the feasibility and value of bringing connectivity to the healthcare industry. The initial phase of the proof-of-concept project was successfully demonstrated on 5 June 2003. Subsequent demonstrations showed the creation

of health topics by data source organizations and the secure transmission of the topics to data review organizations.

The prevailing state for collaboration and data sharing between data source organizations (healthcare service providers including hospitals, physicians and laboratories) and data review organizations (pharmaceutical and medical device companies, government agencies and health insurers) in the healthcare ecosystem at the time of the initiation of the HCN initiative was that of complex mixture of unreliable, untimely and nonstandard modes of communication (Figure 1-1). Information exchange is achieved through means that include mailing of documents through the postal service, faxing of documents and point-to-point electronic exchange of data using e-mail or nonstandard messaging systems. These methods were not only inefficient, costly, and insecure, but also unreliable and untimely.

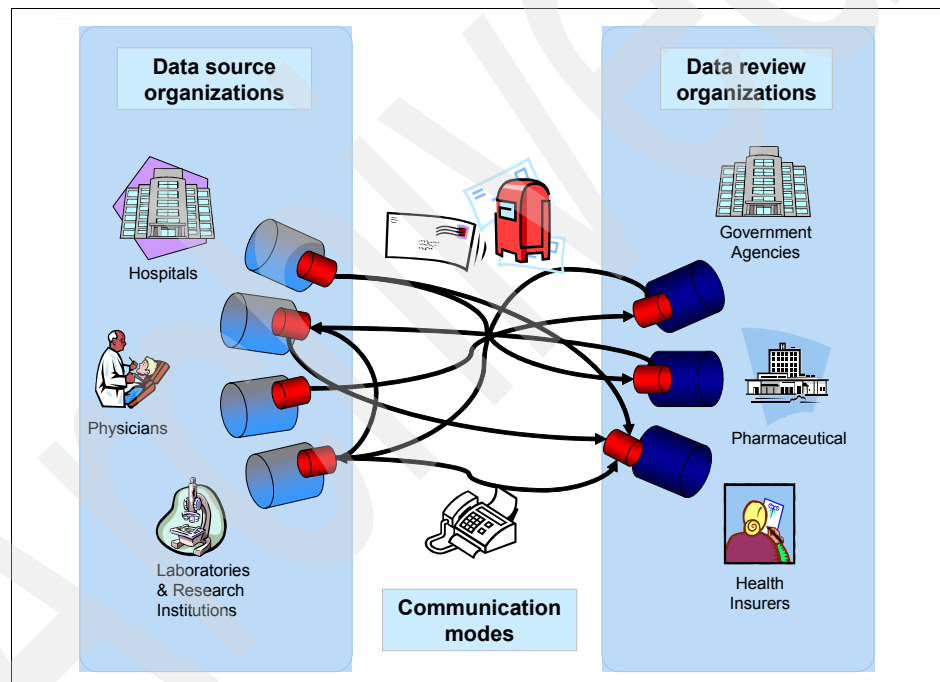


Figure 1-1 Current healthcare data exchange network

In the WebSphere Business Integration for Healthcare Collaborative Network, IBM has developed a product based on open standards designed to address the various shortcomings of the current disparate means for collaborative data exchange identified in the HCN proof-of-concept. The HCN solution enables the dynamic creation of health topics, supports private and highly secure

dissemination of clinical data, and dramatically improves reliability and speed of data delivery.

At a time when the healthcare industry is facing cost escalation and numerous other challenges, HCN is positioned to increase efficiency and reduce costs significantly while also addressing challenges in quality of care, preparedness against infectious disease outbreaks and bioterrorism, and early detection and response to adverse drug effects (Figure 1-2).

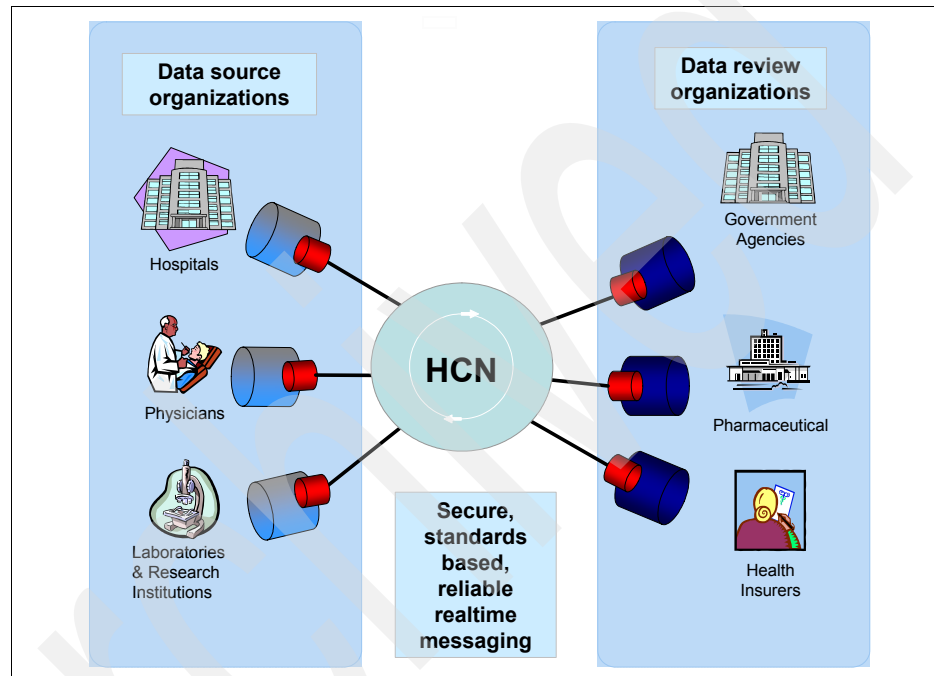


Figure 1-2 HCN standards based collaborative network

1.1.2 Trends enabling Healthcare Collaborative Network

There is an emerging and growing consensus among healthcare stakeholders and consumers alike for the urgent need to improve healthcare services. The momentum is gathering around a number of trends, at the center of which is information technology. The following are some of the emerging trends that are related to HCN:

- **Maturity of technology**

There is significant advancement and maturity in technologies that allow for effective health information exchange. The Internet is mature and advanced enough to create secure wide area networks interconnecting participants in

healthcare ecosystems. Data standards and common medical terminologies for use in communicating clinical data such as HL7, LOINC, and ICD-9 and ICD-10 now exist. Security and privacy is paramount in healthcare. There exist standards and technologies to ensure that appropriate data is made available only to the right people.

- Cost reduction through use of technology

Cost escalation is a major concern in healthcare worldwide. There is a growing consensus that the use of technology to automate processes and improve operational efficiencies can lead to cost reduction in healthcare, as it has in other fields such as finance and manufacturing.

- Bio-preparedness

The presence of the real threat of bioterrorism attacks demands urgent realization of bio-preparedness systems with capabilities that include prevention, diagnosis, early detection, and the management of bioterrorism related conditions. ‘

- Adverse drug reactions

Complications from therapeutic drug courses resulting in morbidity and mortality are common adverse drug reactions. The recent withdrawal and subsequent revelations about the safety of blockbuster drugs is raising the pressure on the pharmaceutical industry. As a result, there is renewed drive to monitor clinical data to track real and potential adverse events.

- Disease outbreaks

Incidents of infectious diseases in humans appear to be increasing. New diseases are appearing in certain populations, and known diseases are spreading to new populations and geographic areas. The threat of emerging diseases such as AIDS, SARS, and Lyme disease, and re-emergence of malaria, tuberculosis and cholera are such that close monitoring for the onset of outbreaks are essential for speedy response to prevent further exposure and infections.

These trends highlight the need and the importance for delivering quality and efficient healthcare through information and information technology and the realization of the need for a collaborative network that can tie it all together.

1.1.3 How Healthcare Collaborative Network works

The fundamental building block for information sharing in HCN is the *Clinical Topic*. A Clinical Topic defines a set of criteria which must be satisfied in the context of a single patient. Clinical messages which meet this criteria, and potentially other messages which describe a complete clinical encounter for the patient, are transferred from Data Source Organizations (publishers) to Data

Review Organizations (subscribers). The criteria can be solely clinical criteria (such as a particular diagnosis, observation, or medication order), or they can also include demographic criteria such as the patient's age or gender. These criteria can be combined in various ways to create Clinical Topics that are as simple or as complex as HCN participants require.

HCN consist of three major components that form the network for exchanging clinical data that are defined as Clinical Topics. These three components form a hub and spoke structure (Figure 1-3).

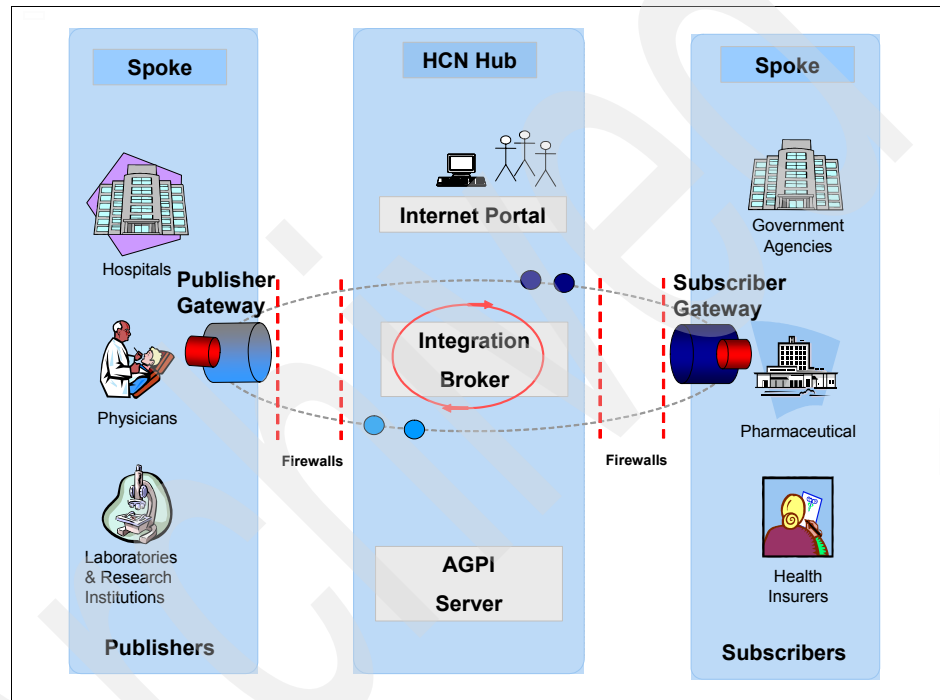


Figure 1-3 HCN hub and spoke structure

The hub

At the center of the data exchange network sits the HCN Hub that consists of the following:

- The Administrative server manages the overall information flow and topics within the system. It supports the creation and configuration of clinical topics that define the criteria for messages to be published and received in the system.

- ▶ The Message Flow server manages the exchange of messages from data source organizations to authorized data review organizations. Routing of the messages is based on Clinical Topics.
- ▶ The Anonymous Global Patient Identifier (AGPI) server assigns anonymous IDs to patients and correlates non-clinical information about patients from different settings to determine when the same person is known by different patient identifiers. AGPI is used for track and matching patients. Installing the AGPI server is optional within the hub or it can be a component that is owned by a trusted third party or government entity.

The spokes

The publisher gateways (installed at Data Source Organizations) and the subscriber gateways (installed at the Data Review Organizations) form the *spokes* in the HCN data exchange network. A gateway is deployed within each organization's IT infrastructure, connecting the organization to the HCN hub. The gateway performs the following functions:

- ▶ Integrates with the Data Source Organization's systems (pharmacy, laboratory, ADT, and so forth) and collects the clinical messages that are needed to select messages against the criteria for Clinical Topics.
- ▶ Correlates and aggregates the required patient data as defined by the Clinical Topic.
- ▶ Transforms the clinical information as required for transmission to Data Review Organizations, for example, by correcting nonstandard usage, up-coding to standard terminology, converting to standard document format, and removal of patient-identifying information from the message.
- ▶ Exchanges messages with the HCN Hub in a highly secure manner to maintain the privacy of the information being exchanged.
- ▶ Integrates with the Data Review Organization's IT systems, providing the data that is required by the Data Review Organization to perform a coherent analysis of the patient information.

Clinical messages

The term *clinical messages* in the context of HCN means *HL7 version 2 messages*. The algorithm that evaluates clinical messages against the criteria of a clinical topic is based on HL7 version 2.4. However, other HL7 2.x versions are supported. In some cases where differences between other HL7 2.x versions and 2.4 are significant, the gateway must be configured to transform the incoming HL7 message to a form that is compatible with version 2.4. In most cases, this is not necessary because V2.4 is backwards-compatible with earlier versions.

For details on HL7, see:

<http://www.hl7.org>

Members of HL7 are allowed to download the HL7 version 2 message specifications and other HL7 standards.

In addition to HL7 v2.x messages, the HCN Publisher Gateway can accept clinical (or other) information in XML documents. However, these XML documents are not evaluated against the clinical criteria of Clinical Topics. Instead, these documents are published to the HCN Hub (and through it to Data Review Organizations) based on the type (XML) of the document.

One particular XML document type is of importance to HCN: the Clinical Document Architecture (CDA) document type that is defined by HL7. A CDA document contains clinical information about a single patient and is intended to contain information that is related to an encounter with a healthcare provider (although the document schema is flexible and can represent information that spans an encounter).

Clinical topics

Clinical topics are the fundamental building blocks of the HCN clinical data exchange. Clinical topics are usually defined by Data Reviewer Organizations, but Data Source Organizations can also create topics for the data they generate. Clinical topics define the set of criteria that are used to determine how clinical data is filtered and packaged for publication. Topics contain the following attributes:

- ▶ Topic name
- ▶ Topic description
- ▶ Topic time limit (duration)

Used to indicate the time-span within which the criteria must occur in order for the topic to be triggered by a set of messages for a patient. For example, you might use a Topic time limit of seven days to indicate that an observation must occur within seven days of a medication order for a particular drug

- ▶ Privacy level

Defines the privacy level associated with the topics. Privacy Levels control how much patient-identifying information is removed from the messages before publication.

- ▶ Patient gender and age filters

Optionally used to indicate whether patients must meet gender or age criteria.

- ▶ Payload information

Indicates the format for messages to be published (CDA or HL7) and also any additional HL7 message types to include when publishing for this topic.

- ▶ Topic Trigger Event

Optional criteria that must be satisfied first (all messages prior to this criteria are ignored when evaluating the topic).

- ▶ Items of Interest

The additional criteria (in addition to the Topic Trigger Event) that must be satisfied for a set of messages to be published under this topic.

To assist you in providing these attributes for topics you create, the HCN Administrative server defines different topic protocols, which default certain attributes depending on the nature of the topic you are creating. The topic protocols that are supported by the HCN Administrative server are:

- ▶ Public Health Alert

The Public Health Alert (PHA) topics are used for reporting cases that are indicative of real or potential outbreaks that pose a risk to the population. SARS and avian flu (H5N1) or terrorist attacks using biological or chemical agents are examples of outbreaks of interest. PHA topics do not require the definition of a *Topic Trigger Event*.

- ▶ Adverse Drug Event

The Adverse Drug Event (ADE) topics are used for reporting cases that are indicative of real or potential adverse events, such as patients who exhibit abnormal lab values after receiving a medication. ADE topics require that you specify a medication and one or more lab values as patient selection criteria. The *Topic Trigger Event* must be Drug Order, and additional criteria can be added to include Lab Test or Observation results, Procedure Orders, or diagnoses.

- ▶ Quality of Care

Quality of Care topics are used mainly to broadly select patients based on a diagnosis or an order for a medication (either a single drug or one of a list of drugs). This kind of topic can be used with a Topic time limit to publish a set of messages as soon as some condition related to the quality of care for those patients occurs (for example, an laboratory or observation result), or can be used without a time limit to publish a set of messages for the patient after the clinical encounter has completed. The data can then be used by the Data Review Organization for more detailed analysis.

► XML Only content for clinical research

The data published by XML only topic types are not evaluated against clinical criteria specified in Clinical Topics. Instead, the Clinical Topic merely indicates that all messages (for all patients) that use a particular XML schema should be published. These topics are used to forward genomic and drug trial data to a Data Review Organization.

The payload options of XML topics allow for the following message types:

- Haplotype Map is used by participants in the HapMap project to send massive compressed XML files that contain the sequence and alleles for each Single-nucleotide polymorphism (SNP).
- MicroArray Gene Expression Markup Language (MAGE-ML) is a language designed to describe and communicate information about microarray based experiments.
- Bioinformatic Sequence Markup Language (BSML) is an open XML data representation and interchange format that enables more efficient communication of genomic research information within the life sciences community.
- Operational Data Model is an XML-based Operational Data Model that provides a format for representing the study metadata, study data, and administrative data that is associated with a clinical trial.

Additional types of XML data can be transmitted using HCN by configuration of the Gateway and Administrative Server.

1.1.4 Benefits of Healthcare Collaborative Network

The willingness of healthcare participants to work together in healthcare ecosystems is beneficial in itself. Making it easier for participants to share clinical data makes it compelling enough to want to take advantage of efficiencies to be gained. HCN features and functions offer significant value to all participants from healthcare providers, clinicians, pharmaceutical companies and payers/health plans to government healthcare agencies.

Benefits to participants

Benefits to participants include the following:

- Healthcare service providers stand to benefit from the alert capabilities of HCN. For example, they are warned when the system encounters patients who are at risk for adverse events. They also benefit from the improved access to clinical information to make informed patient care decisions and monitor quality of care.

- ▶ Pharmaceutical companies can benefit by getting access to de-identified patient data for use in identifying patients for clinical trials, for automated collection of data during trials, and for post-approval alert and analysis of how use of drugs and practice patterns are affecting patients. These benefits add up to reduced costs of sponsoring clinical trials, which allow researchers to focus on identifying and developing beneficial drugs.
- ▶ Government health agencies stand to provide better service to the general public from their improved ability to identify, analyze, respond to, and alert the public of health-related challenges.
- ▶ Health insurers have the opportunity to enjoy reduced costs realized through quality improvement and medical management activities as a result of automated collaborations with healthcare service providers. Additionally, improved quality of care reporting and monitoring for adherence to established treatment protocols can only improve care delivery.
- ▶ Patients, of course, have the most to gain when their care providers have access to relevant clinical information about their individual and family health history.

Data interoperability

HCN was designed to securely transmit healthcare information from publishers to subscribers in real time. By enabling the exchange of data in HCN, the participants do gain a number of benefits beyond subscribing to and publishing of topics. These benefits include:

- ▶ Data standards
 - HCN transmits data using Health Level 7 (HL7) version 2.4, with clinically relevant values defined using accepted coding standards such as:
 - Logical Observation Identifiers and Codes (LOINC)- for laboratory results and other observations
 - International classification of Disease codes, version 9 (ICD-9) for diagnoses
 - Current Procedural Terminology (CPT4) or ICD-9 for clinical procedures

Participants need to map their only local clinical codes to these standards to communicate effectively with fellow participants regardless of their local clinical codes.

- ▶ Data security
 - HCN provides a set customizable security and privacy features to enable participants to meet regulatory restrictions imposed on the handling of healthcare information anywhere in the world. However, out of the box, HCN implements strict privacy and security requirements for data confidentiality, integrity, authentication, authorization, and non-repudiation, using regulations

such as the HIPAA Limited Data Set regulations to determine what patient-identifying information should be transmitted and standards, such as SSL public key encryption protocol.

Configure and run

HCN was designed to enable you to install and have it running as quickly as possible. The three step process of installing, configuring, and running has advantages over the build-scenario where you must undertake additional development before the application is up and running which is found in most healthcare solutions today. Figure 1-4 on page 14 shows the configurable and customizable components of HCN, which are as follows:

- ▶ **Installation and configuration**

Configuration and installation of HCN is quite flexible. If you already running any of the HCN prerequisite applications, you do not have to install them again. Most aspects of HCN are configurable, this has the benefit of enabling you to tailor your HCN installation to your specific needs. Topics and privacy are key features that you can configure practically every aspect of without the need to engage in application development of any sort. These capabilities have significant cost and skills benefits. You can find detailed information about how to install and configure HCN in Chapter 3, “Installation and configuration” on page 93.

- ▶ **Customization**

To accommodate unique circumstances that can emerge with your installation and to ensure that your applications can comfortably interoperate with HCN, the design for HCN is adaptable and as such you can customize certain features of HCN. Customization has the advantage of enabling you to seamlessly integrate HCN to your existing applications. You can find information about customization in Appendix A, “Customizing Healthcare Collaborative Network” on page 181.

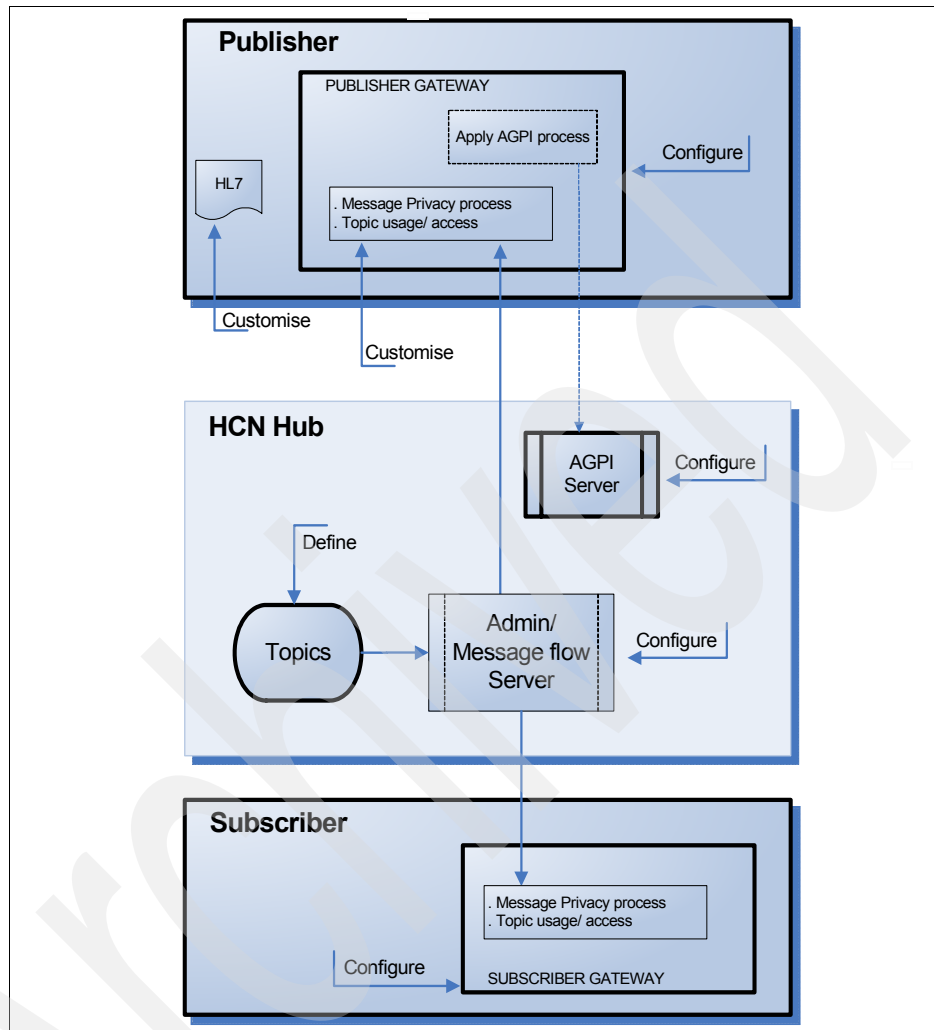


Figure 1-4 HCN configure and run

1.2 Solution models

There are a wide variety of business and deployment models possible with HCN. Ultimately, each of these models reduce to a hub and spoke deployment architecture, with the HCN Hub in the center and Publisher and Subscriber Gateways comprising the spokes. But the differing business and deployment models will dictate different ownership and cost-sharing arrangements, as well as unique security and privacy considerations. Some possible deployment models are:

- ▶ Government Sponsored

In this model, a government (local, regional, or national) owns the HCN Hub. Subscriber organizations are likely to be government agencies (such as public health agencies or government sponsored health plans), although private subscribers, such as researchers, are possible. Government regulations might be used to compel healthcare providers to join the network as publisher organizations.

- ▶ Regional Health Collaboration

In this model, a group of interested parties within a region come together and create a governance structure to facilitate the exchange of health-related information. The parties jointly create a not-for-profit entity to own and administer the HCN Hub. Health insurance plans might be the key subscriber organizations in this model, because of their ability to save money through case management and reduced claims handling costs by having better access to clinical information. *Pay for Performance* incentives might be used to incent participation of healthcare providers. Additionally, providers might be willing to join to receive information from other providers when patients are seen on referral.

- ▶ Academic Medical Research Center

In this model, a large institution, such as an academic medical research center, is the *core tenant* of the HCN solution, acting as administrator of the hub, publisher (through its medical hospital and clinics), and subscriber (through its researchers). Other entities, such as health insurance plans or public health agencies, can join the network to take advantage of better access to clinical information.

- ▶ Independent Delivery Network (IDN)

In this model, a group of hospitals and clinics which are under common ownership, but more-or-less managed independently, can create a collaboration network to facilitate exchange within the IDN. A collaboration solution such as HCN might be seen as easier to implement than aligning the IT systems of many different providers, because the providers might have been acquired over time and might each have their own IT architectures with

unique clinical systems from different vendors. Again in this case, other entities, like health insurance plans or public health agencies, can join the network to take advantage of better access to clinical information.

► Sole Subscriber

In this model, a large entity with a need for clinical information from a variety of sources sponsors the HCN Hub and is the sole subscriber. Examples of a sole subscriber could be a large health insurance plan, which wants data for claims processing and case management, or a pharmaceutical company, which wants data for clinical trial recruitment and assessment. In this scenario, the sole subscriber would likely have to pay providers to join the network and provide clinical data. A slight variation of this is for the sole subscriber to allow other subscribers with similar interests to join the network in exchange for agreeing to offset the expense of maintaining the HCN Hub and compensating providers.

In each of these models, the existence and location of a Master Patient Index (MPI) application to assign a common, anonymous patient ID to patients who are seen by multiple providers, is a crucial requirement. In HCN, a component — the AGPI server — is provided to perform this role. In any particular deployment, the parties might have another MPI application they wish to use. IBM can customize the HCN to interact with another MPI application. However, we describe the use of HCN only with the AGPI server.

In some of these models, it might be desirable for privacy or regulatory reasons to separate the ownership and location of the AGPI server from the rest of the HCN Hub.

This is just a partial list of possible deployment models, and others can be envisioned which combine aspects of two or more of these. It might seem obvious, but it is worth stating: a Chief Information Officer or IT Architect must keep in mind that the business and governance model of the collaboration solution must be determined before the hardware, software, network, and security architecture can be planned.

1.3 Public Health Alert scenario

In our scenario, we use an example of a Public Health Alert to demonstrate the capabilities of HCN. Experts predict that another influenza pandemic is inevitable subsequent to three that occurred in the twentieth century:

- ▶ Spanish flu in 1918
- ▶ Asian flu in 1957
- ▶ Hong Kong flu in 1968

We have chosen a scenario that considers the outbreak of Avian Influenza (Bird Flu) and Avian Influenza A (H5N1). We look at the different stages of a pandemic and show how you can use Healthcare Collaborative Network to facilitate surveillance, rapid exchange of data concerning the start and spread of influenza pandemic, and provide national and international healthcare agencies with ongoing data.

The stages of a pandemic as defined by the World Health Organization shows the progression from interpandemic stage (where no influenza virus are detected in humans) to the pandemic stage (where you have sustained transmission in the general population) as shown in Table 1-1.

Table 1-1 Stages of a pandemic (from World Health Organization)

Period	Phase	Description
Interpandemic	Phase 1	No new influenza virus subtypes have been detected in humans. An influenza virus subtype that has caused human infection might be present in animals. If present in animals, the risk of human infection or disease is considered to be low.
	Phase 2	No new influenza virus subtypes have been detected in humans. However, a circulating animal influenza virus subtype poses a substantial risk of human disease.

Period	Phase	Description
Pandemic alert	Phase 3	Human infection(s) with a new subtype, but no human-to-human spread, or at most rare instances of spread to a close contact.
	Phase 4	Small cluster(s) with limited human-to-human transmission but spread is highly localized, suggesting that the virus is not well adapted to humans.
	Phase 5	Larger cluster(s) but human-to-human spread still localized, suggesting that the virus is becoming increasingly better adapted to humans, but might not yet be fully transmissible (substantial pandemic risk).
Pandemic	Phase 6	Pandemic phase: increased and sustained transmission in general population.

The different stages define a progressively increasing risk for influenza infection. Early detection during the *pandemic alert* stage offer the best chance for containing or delaying the spread of the onset of human influenza. Success depends on preparedness, which includes surveillance, coordination, monitoring and assessment, and realtime communication. HCN is designed to provide the information infrastructure capable of driving preparedness that is coordinated at the global, national and regional levels.

In our example scenario, we adopt an approach that demonstrates one of the attractive features of HCN, the ability to start small and scale the solution to a very large global network without having to redesign your solution. Next, we describe the solution overview for the scenario and throughout the rest of this redbook, we will reference this scenario as we discuss features of HCN.

1.3.1 The scenario

Our scenario most closely resembles the Regional Health Collaboration solution model. It is an independently owned and managed network that facilitates collaboration between different healthcare service providers, government, and international agencies. The network is setup to function as part of an overall and comprehensive pandemic preparedness and response program. It provides surveillance in the pandemic alert stage. and following the onset of a pandemic, it is used for additional purpose of communicating and managing quality of care.

The following are the key functions that this healthcare collaborative network provides:

- ▶ Surveillance

Topics defined in the network are used to capture and to publish incidents which are communicated to subscribers to detect the emergence of new and unusual viruses. For example, circulation of the highly pathogenic avian flu (A/H5N1) is currently spreading in birds starting from Asia and moving westwards to Europe and Africa. Topics are defined specifically to detect the emergence of the pandemic strain that has the ability to transmit from person-to-person.

- ▶ Communication

The network makes use of the HCN capability to facilitate the rapid dissemination of the data from the originating locations (pin-pointing location of new cases) to any national and international organizations that are subscribers to the network.

- ▶ Health system response

Quality of Care (QOC) topics are used to manage order for medication (either a single drug or one of a list of drugs). QOC topics are used with Topic time limit to publish messages related to the care of flu patients. The data can then be used for analysis on the progression and containment of the pandemic.

We started with a very simple model, However, this model can grow to include global scale publishers and subscribers for a worldwide network for pandemic preparedness. The solution is a single site installation consisting of four organizations which include a hospital and a laboratory who publish to the network and a sole subscriber which is a government agency. The network is run by the fourth organization which has administration responsibilities and maintenance of the hub.

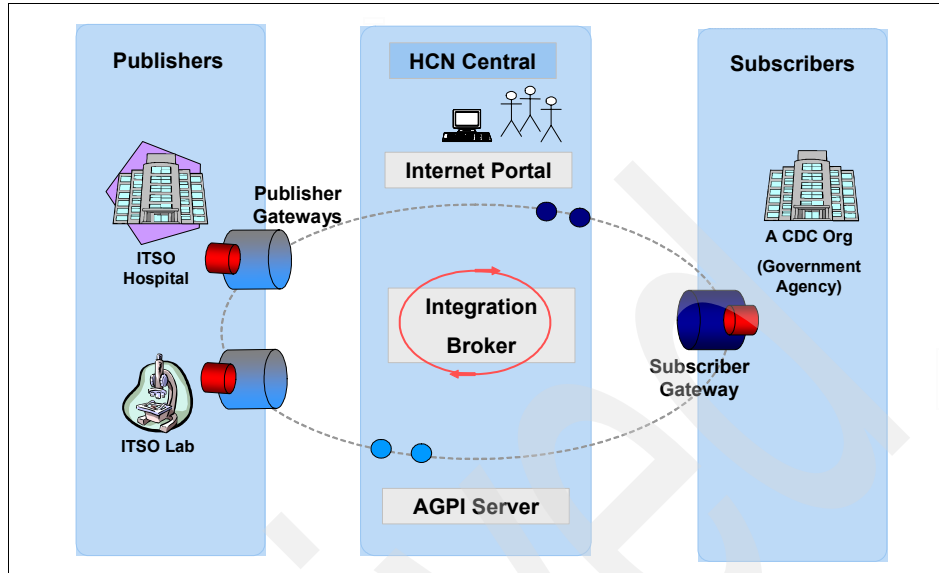


Figure 1-5 The scenario

Note: We designed and installed our example HCN solution in a single site scenario. As a result, we did not have multisite considerations, such as VPN tunnelling and installation of firewalls for security.

1.3.2 Organizations

We created four organizations in the scenario:

- ▶ **HCN Central**
This organization represents a trusted third-party (a non-profit organization, for instance) which owns and administers the HCN Hub for an influenza network.
- ▶ **A Center for Disease Control Organization (ACDCORG)**
This is government public health agency charged with providing health, safety, and essential human services. A Center for Disease Control is a subscriber.

Table 1-2 Attributes of ACDCORG organization

Attribute Name	Attribute value
Organization name	ACDCORG
Privacy level	Fully Identified HIPAALimitedDataSet HIPAAFullyDeidentified
Organization Primary user	acdprimary@itsoacd.gov
Gateway names	ACD_SUBSCRIBER
Users in organization	drlakshmi@itsoacd.gov drnaveen@itsoacd.gov acdgwprimary@itsoacd.gov acdprimary@itsoacd.gov

► ITSO Hospital

A corporation that owns and operates several hospitals, offering a wide range of medical services locally in the communities where it operates.

Table 1-3 Attributes of ITSO Hospital organization

Attribute Name	Attribute value
Organization name	ITSO Hospital
Privacy level	Fully Identified HIPAALimitedDataSet HIPAAFullyDeidentified
Organization Primary user	hospitalprimary@itsohospital.com
Gateway names	HOSPITAL_PUBLISHER1
Users in organization	hospitalgwprimary@itsohospital.com hospitalprimary@itsohospital.com drwerner@itsohospital.com dryuan@itsohospital.com

► ITSO Lab

It is a full-service regional medical laboratory that provides testing and consultation services to hospitals, physicians, and urgent care facilities.

Table 1-4 Attributes of ITSO Lab organization

Attribute Name	Attribute value
Organization name	ITSO Lab
Privacy level	Fully Identified HIPAALimitedDataSet HIPAAFullyDeidentified
Organization Primary user	labprimary@itsolab.com
Gateway names	LABORATORY_PUBLISHER1
Users in organization	mrbrown@itsolab.com drpietro@itsolab.com labgwprimary@itsolab.com labprimary@itsolab.com

1.3.3 Publishers

Two publishers are defined in the scenario and they are:

► ITSO Hospital

A publisher gateway is deployed for ITSO Hospital. The Clinical Information Systems of the ITSO hospital organization send HL7 messages to the HCN Gateway through an Integration Engine in the hospital, using HL7 low-level protocol. The incoming messages are fully-identified. The gateway sends requests to assign an anonymous ID for each patient to the AGPI server in the HCN Hub, which generates the anonymous patient ID. Messages are de-identified prior to being sent to the HCN Message Flow server. Table 1-5 lists the different attributes of ITSO Hospital.

Table 1-5 Attributes of ITSO Hospital publisher gateway

Attribute Name	Attribute value
Gateway Name	HOSPITAL_PUBLISHER1
Gateway Type	Publisher
Gateway Primary user	hospitalgwprimary@itsohospital.com
Gateway Privacy level	Fully Identified HIPAALimitedDataSet HIPAAFullyDeidentified

Attribute Name	Attribute value
Users associated	drwerner@itsohospital.com dryuan@itsohospital.com

► ITSO Lab

The second publisher gateway is deployed for ITSO Lab. The laboratory information system at ITSO Lab sends HL7 messages to the HCN Gateway using HL7 low-level protocol. The incoming messages are identified by the Medical Record Number of the ITSO hospital, which has sent the samples to the lab for processing. The gateway sends requests to assign an anonymous ID for each patient to the AGPI server in the HCN Hub, which returns the anonymous patient ID previously assigned (based on the Medical Record Number). Messages are de-identified prior to being sent to the HCN Message Flow server. Table 1-6 lists the different attributes of ITSO Lab.

Table 1-6 Attributes of ITSO Lab publisher gateway

Attribute Name	Attribute value
Gateway Name	LABORATORY_PUBLISHER1
Gateway Type	Publisher
Gateway Primary user	labgwprimary@itsolab.com
Gateway Privacy level	Fully Identified HIPAALimitedDataSet HIPAAFullyDeidentified
Users associated	mrbrown@itsolab.com drpietro@itsolab.com

1.3.4 Subscribers

We defined only one subscriber in the scenario. ACDCORG is the sole subscriber, and Table 1-7 lists the different attributes for the subscriber gateway.

Table 1-7 Attributes of the ACDCORG subscriber gateway

Attribute Name	Attribute value
Gateway Name	ACD_SUBSCRIBER
Gateway Type	Subscriber
Gateway Primary user	acdgwprimary@itsoacd.gov

Attribute Name	Attribute value
Gateway Privacy level	Fully Identified HIPAALimitedDataSet HIPAAFullyDeidentified
Subscription e-mail ID	drlakshmi@itsoacd.gov
Users associated	drlakshmi@itsoacd.gov drnaveen@itsoacd.gov

1.3.5 The topics

The scenario is designed for use in detecting the onset of influenza pandemic by publishing topics on influenza A (H5N1). Figure 1-6 and Table 1-8 on page 25 show parameters for the definition of the sample topic for detecting influenza A (H5N1). Topics in HCN are dynamic so new topics can be defined to detect other strains of avian flu such as A (H7N7) or A (H9N2).

The dynamic feature of topics can also be used after the onset of a pandemic for communicating and managing Quality of Care. This scenario is designed to support QOC topics which are dynamically created to enable participants in the network to share and mandate effective course of treatment.

The screenshot displays the 'Create Topic Definition' interface. At the top, there's a navigation bar with 'Subscriptions', 'Health Topics', 'Notifications', and 'Gateways'. The 'Health Topics' tab is active. The main form is titled 'Create Topic Definition' and contains several sections:

- Basic Details:**
 - Topic Name:** Influenza A (H5N1) reports (Maximum 50 characters)
 - Topic Type:** Public Health Alert
 - Topic Description:** This topic is concerned with reports of new influenza A (H5N1) cases within the HCN domain. All members of this HCN domain are required to submit any and all suspect H5N1 cases. (Maximum 512 characters)
 - Topic Time Limit:** No limit (radio button selected), 14 days(s), 0 hour(s)
 - Privacy Level:** HIPAA Fully Deidentified (dropdown menu)
- Items of Interest:**
 - Disease Diagnoses:** Add Disease Diagnosis button
 - Lab Test Orders:**

Figure 1-6 Topic creation screen

Table 1-8 Sample Influenza_A_H5N1 topic parameters

Field		Value
Basic details	Name	Influenza_A_H5N1_reports
	Type	Public Health Alert
	Description	This topic is concerned with reports of new Influenza A -H5N1- cases within the HCN domain. All members of this HCN domain are required to submit any and all suspect H5N1 cases. A Center for Disease control -ACD-
	Time limit	No limit
	Privacy level	HIPAA LimitedDataSet
Items of interest	Disease diagnoses	
	Lab test orders	Influenza A AB Test name: Influenza A AB LOINC code(s): 17012-6
	Lab test results	
	Procedure orders	
Patient demographics	Gender	Not applicable
	Age	Not applicable
Payload options	Publish HL7 messages as	HL7
	Include "All" messages of type	<ul style="list-style-type: none"> ▶ Drug Orders ▶ Lab Orders ▶ Lab Results ▶ Admission/Discharge/Transfer ▶ Procedure Orders

1.4 Chapter summary

This chapter introduced HCN and discussed its key features and how it works. It traced the origins of HCN and the trends that enabled the creation of collaborative healthcare networks. It also laid the foundation for usage by presenting solution models and presented an example Public Health Alert scenario that we use in the rest of the book to demonstrate features of HCN.

Archived

Planning and designing your HCN solution

Careful planning is essential for deploying and rolling out your HCN solution successfully. To create your plan, you need to identify the software that you need, and you need to verify the hardware and the network infrastructure to drive your solution.

This chapter discusses the three stages for deploying HCN solutions and identifies the many items that you need to consider to create a comprehensive project plan for realizing your solution. It includes the following sections:

- ▶ Stages of the HCN solution
- ▶ Solution sub-plans
- ▶ Chapter summary

2.1 Stages of the HCN solution

We have divided the deployment of HCN solution into three stages, as illustrated in Figure 2-1:

- Preinstallation

In the preinstallation stage, you analyze your solution scenario, determine the scope of your solution, and identify the different plans that you must create before you commence the installation.

- Installation

In the installation stage, you install and configure the prerequisite software as well as the HCN components.

- Postinstallation

In the postinstallation stage, you test and roll out your solution based on the roll out plan that you developed in the preinstallation stage.

It is imperative that you create a project plan for your HCN solution deployment. A project plan is the one means for ensuring a successful deployment. In this section, we discuss the considerations that enable you to identify the relevant information that you need to create your project plan.

Note: Every HCN solution scenario is unique based on the objectives of the organization. Our goal is not to create a single plan that fits all scenarios but to help you to arrive at a plan that is appropriate for your scenario.

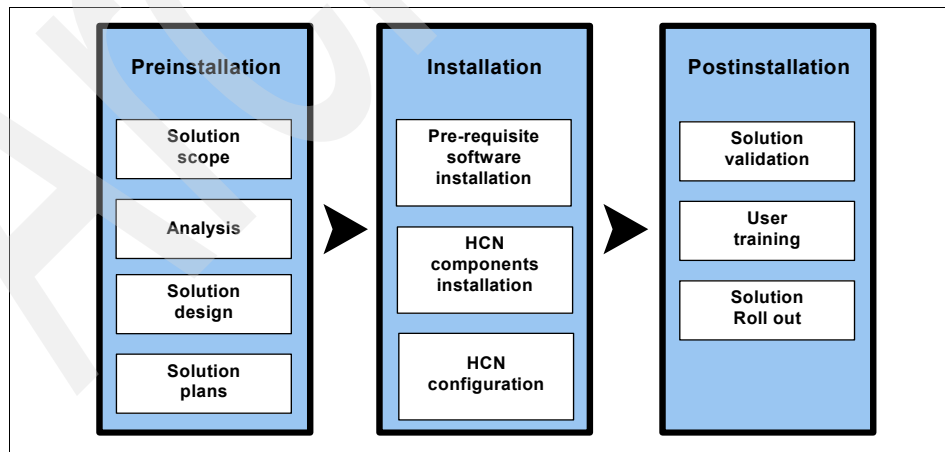


Figure 2-1 HCN solution stages

2.1.1 Preinstallation stage

During the preinstallation stage, you gain a complete understanding of your solution scope and identify all the plans that you need to create for your deployment and roll-out. The following sections discuss the key activities that you have to undertake for this stage of the process.

Solution scope

The ideal starting point for identifying your solution scope is the set of objectives that you set for your HCN solution. These are usually statements about the desired outcome of the HCN solution. The quantifiable aspects of your objectives usually identify the boundary points and the scope for your solution.

Solution scope considerations include the following:

- ▶ Number of sites

You need to consider the number of sites for your solution. If this is a multi-site and multi-organization solution, you might consider limiting the initial scope of the deployment and adopting a phased approach where you can add new sites with subsequent deployments.

- ▶ Users and user roles

You need to define the number and types of users for your solution. User scope considerations include the roles, necessary training and education, your deployment and roll out strategy, and ensuring consistency with your solution goals and objectives.

- ▶ Topics

Health topics are central to HCN support for exchange of clinical data. To ensure that not only the right topics are published but also that the level of data meets your requirements, you need to take into consideration the different organizations in your network, the topic parameters, and the privacy policy for each topic.

- ▶ Data interoperability

The healthcare industry supports various data protocol standards, however different vocabularies and terminologies make transmitting information a challenge. Understanding the level of data interoperability that is required for your solution to function effectively will enable you to set the appropriate scope and time frame for your solution.

- ▶ Deployment and roll out strategy

Your deployment and roll out strategies are two key scoping considerations for your HCN solution. You have to decide how many nodes to deploy and how to roll out the deployment (phased or simultaneous deployment). Note

that your deployment strategy can impact your overall project scope and other planning decisions significantly.

Solution scoping has the added benefit of driving the remainder of your planning process. The solution's scope helps you can make certain that you are on course for a successful deployment and validates that the solution meets the desired objectives.

Analysis

Before engaging in any project planning, you need a complete understanding of your solution scenario, including the following analysis:

- Information technology infrastructure

You need to analyze your current information technology infrastructure, including a software, hardware, and network analysis. HCN solution components require prerequisite middleware applications. Your software analysis determines whether you have this software with the appropriate licenses. If that is the case, you need to acquire only the HCN solution software. See the IBM product announcement for details:

<http://www-306.ibm.com/fcgi-bin/common/ssi/ssialias?infotype=an&subtype=ca&appname=Demonstration&htmlfid=897/ENUS205-007>

Your hardware assessment determines whether your existing information technology infrastructure meets the hardware requirements for installing the HCN components.

You also need to analyze your network infrastructure. A secure network connecting the HCN hub to the gateways is required for transmission of clinical data.

The flowchart in Figure 2-2 on page 31 gives a high-level overview of the steps that are involved in the HCN analysis.

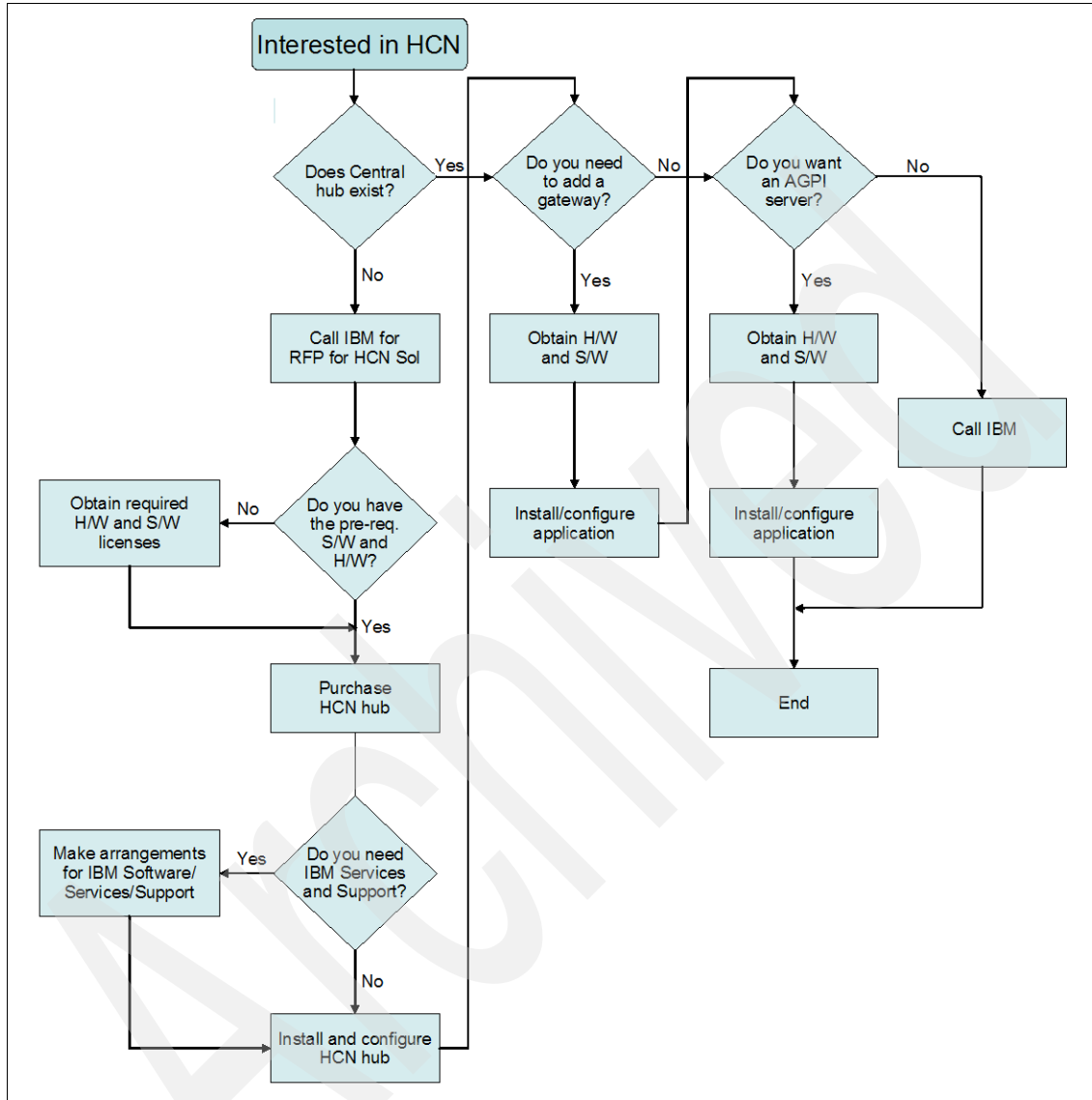


Figure 2-2 HCN analysis overview

► User skills

Ensuring that you have the right skills in your organization is essential for the deployment and day-to-day operation of your HCN solution. As a result, skills assessment is one of the important steps in HCN solution planning. The project team should have the skills to perform the installation, configuration, and postinstallation. Your system operations team should have the skills for

the continued operation of the system. Familiarity with the prerequisite software as described in 2.2.2, “Planning for software” on page 45 is important. Additionally, skills in the following areas are also required:

- Java™ and Python programming knowledge
- SQL experience and basic understanding of relational databases and SQL statements, triggers and stored procedures
- A thorough understanding of your clinical IT systems
- A good working knowledge of HL7 and industry standards for coding clinical data (LOINC, ICD-9, CPT4)

Note: It is recommended strongly that you involve the IBM WebSphere Business Integration services team for training and other installation assistance if you do not have the appropriate skills in your organization.

In addition to the project and operation teams skills assessment, you should also assess the skills of your staff who will use the HCN solution on daily basis. The result of these assessments will help you to create your education plan (see 2.2.1, “Planning for education” on page 42).

► Data interoperability

Information is exchanged routinely in the healthcare industry, often between systems in a given institution such as the lab and the pharmacy in a hospital, as well as across institutions, for example between hospitals and government agencies. Few healthcare institutions share a common vocabulary. For example, Hospital 1 might refer to a heart attack as an *acute myocardial infarction*, a research lab might refer to a heart attack as an *AMI*, and Hospital 2 might refer to the a heart attack as *congestive heart failure*.

HCN processes HL7 version 2.4 messages and LOINC, ICD-9, and CPT4 vocabularies. HCN has the capability to handle different vocabulary, however this needs to be planned for. You have to analyze your nomenclature and plan appropriately for customization (see 2.2.5, “Planning for data interoperability” on page 55).

Solution design

By creating your solution design, you define the physical architecture of your HCN solution. The design is driven largely by the requirements for your solution and the result of your information systems analysis. It undoubtedly conforms to the hub and spoke architecture of HCN, with a single centralized hub and gateways in every publisher and subscriber organization in the network. Critical to your solution design is the purpose for the HCN network (for example, adverse drug event reporting, public health alert reporting, quality of care reporting or health information interchange) and the topics that must be published in order to

meet the goals of the solution. This should form the overarching requirement for the solution design. Finally, the solution design should be bound by the solution scope that you defined.

The hub

Every HCN solution has a single instance of the hub. This simplifies the design, but you still have to consider where to locate the hub, the security infrastructure (firewalls etc) and the administration of the hub. Another decision that you have to consider for the hub is the implementation of the AGPI server. HCN design allows for either a locally installed AGPI server or a remote AGPI server which can be operated by a service provider or other trusted third-party.

Organizations

Publishers and subscribers in an HCN network are represented as organizations. You need to establish operating guidelines and governance for organizations joining the network must conform to. Coupled with the guidelines are considerations that should enable you to arrive at a solution design that meets your HCN goals and objectives, as follows:

- ▶ Gateways

You have to identify the data source organizations and the data review organizations in your network. Publisher gateways will have to be installed and configured for each data source organization and subscriber gateways for data review organizations. Some organizations can be both data source and reviewers, in which case a combined publisher/subscriber gateway will have to be configured for those organizations.

- ▶ Privacy levels

You have to define the privacy levels for each organization to ensure that the appropriate data is published and received.

- ▶ Security

Considerations for security include intrusion prevention using firewalls installed at each organization, and secure electronic messaging (see Chapter 6, “Privacy and security” on page 165 for detail information about privacy and security in HCN).

- ▶ Users

User considerations should identify the different user roles for each organization including designating the primary user for each organization.

Gateways

For each gateway, you must determine how the gateway incorporates with the organization's existing IT systems. Some scenarios might require a custom connector.

For a publisher gateway, the HCN Gateway software can receive clinical messages in a file, via the HL7 low-level protocol, or over a WebSphere MQ queue. For the vast majority of cases, these options will be sufficient to allow the desired communications.

For a subscriber gateway, there are three options for sending data to the Data Review Organization:

- ▶ As HL7 messages using the HL7 low-level protocol.
- ▶ By parsing the HL7 messages and storing data from specific HL7 fields into a relational database. In this case, the exact fields to be stored in the database can be varied, depending on the fields that are of interest to the subscriber.
- ▶ As HL7 messages using the Public Health Information Network (PHIN) protocol that was developed by the United States Center for Disease Control and Prevention (CDC). This option is not described further in this redbook.

This variability in what subscribers can do with HL7 messages is one of the reasons that the Gateway is based on the IBM WebSphere Business Integration server software. WebSphere Business Integration provides connectors that allow it to transfer data to a wide variety of target applications. If a connector does not exist for a particular application being used by the subscriber, a custom connector can be developed using tools included with WebSphere Business Integration. In addition to connectors, WebSphere Business Integration allows data maps to be written to transform messages from one format (in this case, HL7) to other formats (perhaps XML or a specific relational database schema).

The Gateway software does not include any custom application connectors or data maps. They can be created by the subscriber organizations to meet their specific and desired needs.

Topics

Topics are the fundamental building blocks for data publishing in HCN. When you define a topic you specify particular characteristics such as a particular disease state, a particular laboratory result or other observation, the dispensing of a particular medication, or any combination of such characteristics. Your solution design will have to consider what health topic parameters will be needed to answer the intended clinical questions and the analysis that you need to perform. Note that topic definition is dynamic, you can define new topics at any time. However, you cannot retroactively process publications in order to capture new information, so you must give careful consideration to the types of data you need and the analysis you have to perform as you go about defining your initial set of topics.

The following examples of topics show how different parameters can be used in data collection:

- ▶ Patients with a diagnosis of Acute MI
- ▶ Patients with a diagnosis of Acute MI and a prescription for atenolol
- ▶ Patients with a diagnosis of Acute MI, a prescription for atenolol or labetalol, and a lab order for white blood cell count.
- ▶ Patients with a diagnosis of Acute MI and a prescription for at least two of the following: a beta blocker, an anticoagulant, and an ace inhibitor

Solution plans

Before delving into the elaborate task of installing and configuring the different HCN components, you need to create a set of solution plans. Solution planning is the process by which you verify that you have all that you need to install and configure your HCN solution. What you create are sub-plans for specific tasks which you will add to your overall project plan. Note that it might be necessary for you to create additional plans for your solution. For detail description of these plans, see 2.2, “Solution sub-plans” on page 42. The following are the set of plans that we have identified:

- ▶ Education, which includes the steps for bridging identified skills gaps from the analysis you performed in “Analysis” on page 30.
- ▶ Software, which identifies the prerequisite software and HCN components that you need. Your software plan will also ensure that you have all the necessary fix packs for a successful HCN installation.
- ▶ Hardware, which identifies the physical servers and client machines (including machines for your end users) that you need for your solution.
- ▶ Networking, which includes steps to ensure that you have the appropriate network infrastructure to meet your solution needs.
- ▶ Data interoperability, which identifies the local clinical codes that need to be mapped to the HCN standard vocabularies. See Appendix A, “Mapping local clinical codes” on page 203 for information about how to map local clinical codes.
- ▶ Performance improvement, which you can achieve by tuning the HCN solution appropriately. The performance plan identifies the steps that you have to take to tune your solution for optimal performance.
- ▶ Privacy and security, which are essential for correct functioning of HCN. The plan identifies the necessary steps for securing your solution.
- ▶ Plan for service and support, which ensures continued day-to-day operation of your HCN solution.

2.1.2 Installing the HCN

Installing the HCN is the most important activity in getting your solution up and running. Having a plan makes this task seemingly daunting task rather easy to execute. We have identified three installation subtasks of installing the prerequisite software, installing the HCN components, and configuring the entire solution. The output of your solution scope definition, analysis, and solution design from the preinstallation are all inputs towards planning for installation.

Prerequisite software

In the preinstallation phase, you performed system analysis of your software and hardware infrastructure. The result of the analysis and the solution design should identify the following:

- ▶ What you need
 - The machines for running the hub and the gateways
 - Licenses for operating systems and prerequisite software
 - Which if any of the HCN prerequisite software you do not already have
 - HCN components that you need (will depend on the type of solution you are deploying. For example if you are adding a subscriber organization to your network, then the only component you need is the gateway)
 - Fix packs for the operating systems and the prerequisite applications
- ▶ What to install
 - New operating system installation or update to the installed operating system
 - Prerequisite software (if it is not already deployed in your infrastructure)
 - Fix packs to apply to the operating system and the prerequisite applications
 - The hub (Admin server, Message Flow server and AGPI server) and the gateways (publisher, subscriber or publisher/subscriber)
- ▶ Where to install
 - The exact location where to install the hub and the gateways
 - Which machines need new/upgrade to the operating systems
 - Which fix packs to apply for the operating system and the prerequisite applications

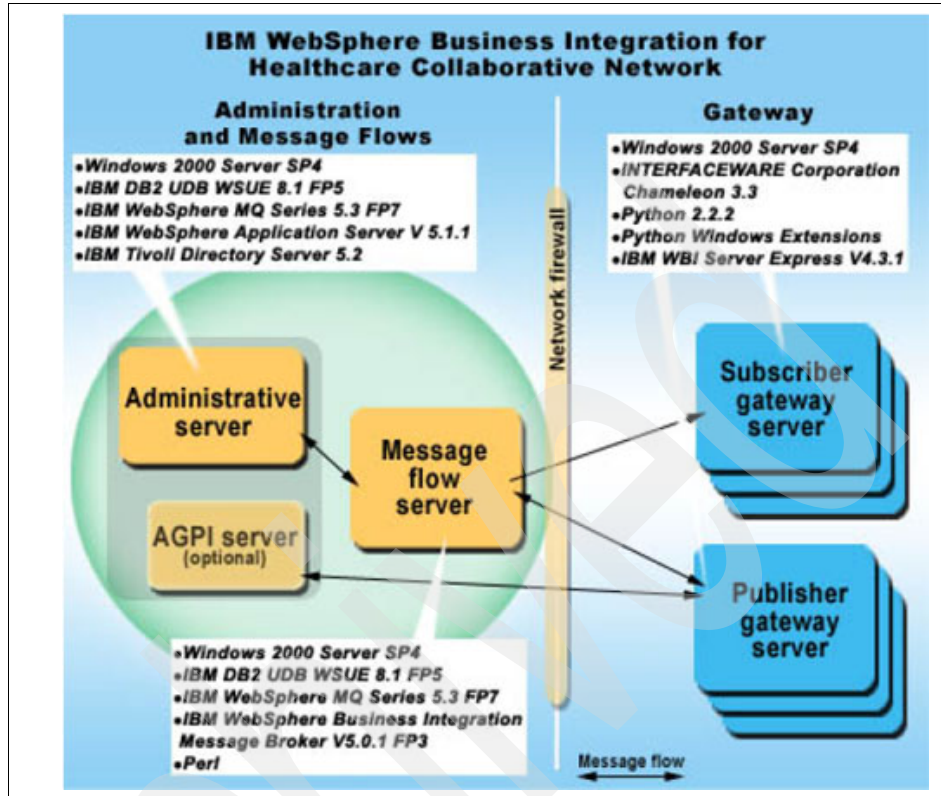


Figure 2-3 HCN prerequisite software

Solution plans in 2.2, “Solution sub-plans” on page 42 provide planning considerations that you need for installing the prerequisite software.

Installing the HCN components

Installing the HCN solution requires that you install the prerequisite software first and then follow that with the installation of the HCN components. Planning for the installation of the HCN components is based on the assumption that you have already created the plan for installing the prerequisite software. HCN components installation is a really simple task, you basically have to decide on which machines to install the components.

You should plan for the installation of the Administrative server, the Message Flow server, and the AGPI server on the machines designated for the hub. Also, you should install the HCN Gateway on the machines that are designated for the publisher, subscriber, and publisher/subscriber gateways. An important aspect of installing the HCN components is the sequence in which the components are

installed. Your plan for components installation must ensure that the proper sequence is maintained especially if you are deploying a large multi-site solution (see 3.2, “Installation requirements and prerequisites” on page 64 for details).

HCN configuration

Upon successful installation of the prerequisite software and the HCN Components, your solution still needs to be configured for optimal operation. Configuring an HCN includes the following tasks:

- ▶ Configuring the hub
 - Assign the administrator
 - Create the HCN entities in the hub (organizations, gateways, and the users)
- ▶ Configuring the gateways
 - Assign names and IDs
 - Assign primary user and users
- ▶ Security configuration
 - Assign the different user roles
 - Assign policy levels to organizations, gateways, and topics (usually done at entity creation time, the planned task might simply be verification of what was created)
 - Decide on self-signed certificates or use a third-party software, such as Verisign
 - Certificate issuance
- ▶ Customization
 - Map local clinical codes
 - Modify or extending the predefined codesets
 - Customize HCN privacy rules
 - Modify existing privacy levels

Planning for gateway configuration requires careful tabulation and tracking of names, IDs, and users. Prior planning can only make the actual configuration tasks easier to carry out. Note that any customization that you deem necessary for your solution is actually further configuration to enable your solution to meet your requirement.

2.1.3 Postinstallation

After you have completed the installation and configuration, you are ready to commence the postinstallation stage. In this stage, you validate your solution, train your users and roll out your solution. We identified some considerations to help you plan for the postinstallation stage.

Validating the solution

Of course, following any installation, you need to validate the solution to be sure that the installed solution is working as expected. It is also the time to tune the solution for performance and test handling of expectations conditions.

Note: We are concerned here with validation of the HCN components and not that of the prerequisite software. You should plan to conduct the validation and proper functioning of the prerequisite software as part of the prerequisite software installation prior to embarking on the HCN components installation.

The set of tests that you can perform to validate your solution are varied. They can be as simple as making sure that you can start the hub and the gateways, to more detail and technical tests involving message queues.

The following are broad areas that we have identified that you need to plan for in order to validate your HCN solution:

- ▶ System power up and down
You need to validate that all the different component of your HCN solution can be powered up and shut down effectively.
- ▶ HCN connections
You validate the HCN connectors and the integration between HCN and your applications.
- ▶ Security
HCN makes use of SSL to ensure secure transmission of messages. Security is at the heart of the value of HCN. Thus, validating that the security function is operating as expected is essential to your deployment.
- ▶ Messaging
WebSphere MQ is used to transmit information in HCN. Validating the message flow through the various queues is one way to ensure that your HCN solution is performing the basic function of sending messages through the HCN.

► Data flow

An end-to-end flow of messages — from the publisher hospital system through the publisher gateway to the publication of messages which are sent by the message flow server to subscribers via the subscriber gateway — is an essential step in validating your solution. You should consider exercising your solution by publishing different topics, sending messages and notifications (both through messages and e-mail), using different privacy levels to ensure that only the appropriate topics are published and sent to the appropriate subscribers. You should devote sufficient time to data flow validation in your plan prior to rolling out the solution.

User training

One of the assessments you had to perform in the preinstallation phase was that of user skills to ensure that you have the right skills for the deployment and day-to-day running of HCN. The success of your HCN solution is dependent, to a large extent, on how well your staff can effectively use HCN, which in itself depends on the quality of the training that is provided. So, in this postinstallation phase, you plan for the necessary training and close the identified skill gaps.

Note: You should coordinate your installation phase scheduling with that of your training so that your users are trained and ready for the solution rollout, especially in instances where you are deploying HCN for the first time.

Your plan for training should include the following considerations:

► The number and type of users

For each user type, a well-conceived training program should be put in place. The HCN user roles is a good starting point for defining the types of users. HCN roles define the privileges afforded to users and the tasks users are authorized to perform. The following are the defined user roles in HCN:

- Administrator
- Primary user
- Observer
- Subscriber
- Publisher

► The setting

The considerations include when and where the training will take place. You should also consider the scheduling of the training making sure that it does not disrupt your normal operation.

- In a classroom setting, ideal for initial training where the users are new to HCN.
- Computer based training, ideal for on-going training where the users are familiar with HCN but need to brush up on the features.

► Approach

- Pilot training

You might consider running a pilot training program to assess and fine-tune the training before rolling the training out to the rest of your organization.

- Direct training with outside instructors

You have the option of offering the training directly using outside instructors for the entire training programs.

- Train-the-trainer

You use outside instructors to train a select set of instructors who then take the responsibility of training the remainder of the users.

Note: Because of the sensitive nature of some of the data that is handled in HCN, it is advisable that you provide special training on security and privacy for all your users.

Solution roll out

The rollout plan is a major part of your overall HCN deployment project plan. It defines your strategy, the resources and responsibilities for deploying your HCN solution. It includes the following elements:

- The verification that your HCN solution is actually ready for deployment. It ensures that you have performed solution validation as part of your postinstallation activities.
- Verification that the skill gaps and staff are trained and ready to use and support the HCN system.
- Verification of the readiness of all organizations and sites to accept the delivery of HCN solution.
- A contingency plan and appropriate risk mitigation procedures.

Additional Considerations

Your HCN deployment and rollout can impose anxiety and stress on your staff. Minimizing the impact on your staff and your overall business routine is essential for the success of your HCN solution. Your rollout plan and strategy should take these into consideration. You should also plan for how to handle unforeseen glitches that might crop up during the rollout.

Additionally, you need to consider planning for the continued operation of your HCN solution:

- ▶ **Availability and continuity**

It is our recommendation that you put in place a plan for non-stop operation of your HCN solution and environment. See 5.4.3, “Backup and recovery” on page 162 for more information about implementing backup and recovery for HCN.

- ▶ **System management**

You should also consider putting in place the plans for the maintenance and management of your HCN solution (see Chapter 5, “System management” on page 147).

2.2 Solution sub-plans

This section introduces the sub-plans that we have identified and discusses the purpose and benefits of those sub-plans. Each sub-plan is modular in nature. They identify the set of individual topics that you need to address and provide more detail information and considerations on the particular topic. The considerations for each sub-plan enable you to verify and validate the topic in question within the context of your solution.

2.2.1 Planning for education

Your skills analysis in the preinstallation stage identified skills gaps in your organization for the HCN deployment project team, the HCN systems operations team and your day-to-day HCN users. This sub-plan is the education plan for addressing the identified skills gaps needed to install, configure, customize, administer and use HCN.

An education plan outlines the different approaches for closing the skills gap. You can adopt one or more of these approaches. Which plan you adopt depends largely on the skills and training that you want your staff to have. The different approaches include the following:

- ▶ Formal education

This includes formal instructor lead classroom training and can be augmented or replaced by self-study programs. You adopt this approach when you want your staff to be and highly skilled and certified in the all the prerequisite software and HCN solution.

- ▶ On-the-job training

With this approach, you engage skilled resources from outside your organization (such as global services for IBM) to work on site to guide your project team and provide guidance working side-by-side with your staff.

- ▶ Outsourcing the work

This approach offers the least in terms of skills transfer. You in effect engage consultants to install and configure and all tasks deemed appropriate to get your HCN solution up and running.

Before you begin

Before you begin, do the following:

- ▶ Identify the skills gaps for installing, configuring, customizing, administering and using HCN in your organization.
- ▶ Decide on the level of skills you want your staff to have and the approach or combination of approaches for training.

Note: We assume that your organization will adopt a formal education approach as the means for bridging identified skills gaps, which implies that the skills are required in-house for installing, configuring, customizing, and administering HCN. Other approaches require only a subset of the tasks described in this section.

Education planning tasks

The following lists the education planning tasks:

- ▶ Project deployment and customization teams education
 - Identify the IBM education road map courses for deployment and development using the prerequisite software.
Ensure that the course availability dates matches your overall project plan to have the skills available for planned tasks.
 - Establish the number of your staff that you want to take the training.
You should have, at the very least, two people who should acquire the needed skills.
 - Ensure that the identified staff have the minimum level of skills required for the training.
 - Contact IBM and book for the prerequisite software deployment and development training.
 - Contact IBM to arrange for formal HCN customization training specifically for your organization.

Note: Note that IBM currently does not offer prescheduled formal courses for HCN. You will have to contact IBM to have training for HCN custom designed and offered for you

- ▶ Systems operations team education
 - Identify the IBM education road map courses for administration using the prerequisite software.
Ensure that the course availability dates matches your overall project plan to have the skills available for planned tasks.
 - Establish the number of your staff that you want to take the training.
You should have, at the very least, two people who should acquire the needed skills.
 - Ensure that the identified staff have the minimum level of skills required for the training.
 - Contact IBM and book for the prerequisite software administration training.
 - Contact IBM to arrange for formal HCN administration training specifically for your organization.

- ▶ User education
 - Identify the members of your staff who should function as the HCN administrator
 - Identify the members of your staff who should function as the primary users for each of the HCN gateways
 - Identify the members of your staff who would use HCN on a daily basis.
 - Contact IBM to arrange for formal HCN user training specifically for your organization.

2.2.2 Planning for software

Software installation is the most important aspect of your HCN solution deployment. Making sure that you have every piece of software, the correct version and the right fix packs is the first step. You must also install then in the right order and validate that every piece you install is functioning before installing the next. This sub-plan is a guide to enable you to create a plan prior to embarking on software installation.

Planning for Windows operating system

Before installing the prerequisite software and the HCN components, you have to load Windows® operating system or verify that your Windows installation is up to date.

Note: The base operating system for HCN components installation is Microsoft® Windows 2000 Server with Service Pack 4 that is updated with the latest security patches from Microsoft.

Before you begin

Before you begin, you need to:

- ▶ Identify the operating system version and releases to be installed.
- ▶ Determine which machines you need to install or upgrade the Windows operating system.

Windows installation tasks

The Windows installation tasks are as follows:

- ▶ Install or upgrade the Windows 2000 operating system.
- ▶ Apply Service Pack 4.
- ▶ Apply all the latest security patches.

After you finish

After you complete the installation process, you need to verify that the operating system version and service packs installed successfully.

Planning for the Administrative Server

Before you can install the Administration Server, you must have installed the Windows 2000 operating system with Service Pack 4 and all the latest security patches.

Before you begin

Before you begin, you need to:

- ▶ Determine where to install the Administration Server.
- ▶ Ensure that the operating system and hardware meet the minimum requirements for the Administration Server.

Administrative Server installation tasks

The Administrative Server requires the following prerequisites and fix packs:

- ▶ IBM DB2® Universal Database™ Workgroup Server Unlimited Edition V8.1 Fix Pack 5 at:
<http://www.ibm.com/software/data/db2/udb/support/downloadv8W32fp5.html>
- ▶ IBM WebSphere MQ 5.3 Fix Pack 7 at:
<http://www.ibm.com/software/integration/mqfamily/support/summary/>
- ▶ IBM WebSphere Application Server Base V5.1.1 at:
<http://www.ibm.com/software/webservers/appserv/was/support/>
- ▶ IBM Tivoli® Directory Server 5.2 at:
<http://www.ibm.com/software/tivoli/products/directory-server/>

After you finish

After you complete the installation, you need to record your Administration server installation information.

Planning for the Message Flow Server

Before you can install the Message Flow Server, you must have installed the Windows 2000 operating system with Service Pack 4 and all the latest security patches.

Before you begin

Before you begin, you need to:

- ▶ Determine where to install the Message Flow Server.

- ▶ Ensure that the operating system and hardware meet the minimum requirements for the Message Flow Server.

Message Flow Server installation tasks

The Message Flow Server requires the following prerequisite software and fix packs:

- ▶ IBM DB2 Universal Database Workgroup Server Unlimited Edition V8.1 Fix Pack 5 at:

<http://www.ibm.com/software/data/db2/udb/support/downloadv8w32fp5.html>

Note: You can use IBM DB2 Universal Database Version 8.1 for WebSphere Business Integration Message Broker. Install the appropriate Fix Pack 5 for the version of DB2 that you selected.

- ▶ IBM WebSphere MQ 5.3 Fix Pack 7 at:

<http://www.ibm.com/software/integration/mqfamily/support/summary/>

- ▶ IBM WebSphere Business Integration Message Broker for Windows XP/2K V5.0.1 Fix Pack 3 at:

<http://www.ibm.com/software/integration/mqfamily/support/summary/>

- ▶ Perl at:

<http://www.activestate.com/Products/ActivePerl/>

After you finish

After you complete the installation, you need to record your Message Flow Server installation information.

Planning for the AGPI Server

Before you can install the AGPI Server, you must have installed the Windows 2000 operating system with the Service Pack 4 and all the latest security patches.

Before you begin

Before you begin, you need to:

- ▶ Determine where to install the AGPI Server
- ▶ Ensure that the operating system and hardware meet the minimum requirements for the AGPI Server.

AGPI Server installation tasks

The AGPI Server requires the following prerequisite software and fix packs:

- ▶ IBM DB2 Universal Database Workgroup Server Unlimited Edition V8.1 Fix Pack 5 at:

<http://www.ibm.com/software/data/db2/udb/support/downloadv8W32fp5.html>

Note: You can use IBM DB2 Universal Database Version 8.1 for WebSphere Business Integration Message Broker. Install the appropriate Fix Pack 5 for the version of DB2 that you selected.

- ▶ IBM WebSphere MQ 5.3 Fix Pack 7 at:

<http://www.ibm.com/software/integration/mqfamily/support/summary/>

After you finish

After you complete the installation, you need to record your AGPI Server installation information.

Planning for the Gateway

Before you can install the Gateway, you must have installed the Windows 2000 operating system with the Service Pack 4 and all the latest security patches and the Administration Server.

Before you begin

Before you begin, you need to:

- ▶ Determine all the locations where you want to install the Gateway.
- ▶ Ensure that the operating system and hardware meet the minimum requirements for the Gateway.

Gateway installation tasks

The Gateway requires the following prerequisite software and fix packs:

- ▶ INTERFACEWARE Corporation Chameleon 3.3 build 83 or later 4 Planning and Implementation Guide at:

<http://www.interfaceware.com/>

- ▶ Python 2.2.2 at:

<http://www.python.org/2.2.2/>

- ▶ Python Windows Extensions (pywin32) build 202 at:

http://sourceforge.net/project/showfiles.php?group_id=78018

- ▶ IBM WebSphere Business Integration Server Express V4.3.1, including the toolset. Required updates for components in the IBM WebSphere Business Integration Server Express V4.3.1 bundle include the following:
 - IBM WebSphere Business Integration Adapter for JDBC™ (no updates)
 - IBM WebSphere Business Integration Adapter for JText (no updates)
 - IBM WebSphere Business Integration Adapter for Web services (no updates)
 - IBM WebSphere Business Integration Adapter for WebSphere MQ (no updates)
 - Java compiler SDK 1.3.1 (required for compiling customer-generated maps and collaborations)
 - IBM WebSphere MQ 5.3 Fix Pack 7 at:
<http://www.ibm.com/software/integration/mqfamily/support/summary/>
 - IBM DB2 Universal Database Express Edition V8.1 Fix Pack 5 at:
<http://www.ibm.com/software/data/db2/udb/support/downloadv8W32fp5.html>

After you finish

After you complete the installation, you need to record installation and location information for all Gateways.

2.2.3 Planning for hardware

Your HCN solution requires hardware on which to run on. It is essential that you have a plan to making sure that you can deploy each HCN component in your solution design. Your hardware planning ensures that can meet all of your hardware requirements whether you acquire new hardware or use existing hardware. Your hardware plan should also include media plan for backup and recovery.

Note: Note that the requirements that are stated in the *Planning and Implementation Guide* are just the minimum requirements. You can find this guide at:

<http://publib.boulder.ibm.com/infocenter/imshelp1/v3r0/index.jsp?topic=/com.ibm.hcn.doc/hcn.html>

Based on the volume of the data flow and the usage, your hardware requirement might be significantly different from the minimum that stated for the base HCN solution deployment.

General hardware planning

Your hardware planning should include a general plan and specific plans for the Administrative, Message Flow and AGPI Servers as well as the Gateways. We start with the general hardware planning and then follow that with the planning for each of the servers.

Before you begin

Before you begin, you need to:

- ▶ Have a list of possible locations.
- ▶ If you plan to use any existing machine, identify the machines and gather their current configuration.
- ▶ Record available disk capacity.
- ▶ Record your current backup and recovery plan detailing your media needs.

General hardware tasks

General hardware tasks include the following:

- ▶ Plan for physical site
 - Create a step-by-step process for ensuring that you have a safe and secure physical site for the server.
 - Make sure that you have the right power and server cabling.
- ▶ Plan for physical disk
 - Shared disk subsystem with RAID.
- ▶ Plan for backup or recovery media
 - Decide on the type of backup/recovery media (for example, tape or optical).
- ▶ Plan for high availability
 - Microsoft certified cluster machine.
 - Mirrored 18 GB boot disk.
 - Mirrored 2x36 GB shared disk.

After you finish

After you complete the tasks, you need to:

- ▶ Record location and physical information.
- ▶ Calculate how much tape or optical media you need for your backup plan.

Hardware planning for the hub

The hub consists of the Administration Server, the Message Flow Server and optionally the AGPI Server. Planning for each of the three servers is quite similar though the hardware requirements differ.

The hub is the central piece of the HCN solution. You should prepare a secure and clean space for the physical location to house the hardware for the different servers that make up the hub.

Before you begin

Before you begin, you need to:

- ▶ Create a list of possible locations where to deploy the hub.
- ▶ If you plan to use an existing machine, identify the machine and gather its current configuration.
- ▶ If you plan to acquire new machine, specify the minimum configuration.
- ▶ Record available disk storage.

The hub hardware tasks

The hub hardware tasks include the following:

- ▶ Plan for physical site.
 - Create a step-by-step process to ensure that you have a safe and secure physical site for the servers.
 - Make sure that you have the right power and server cabling.
- ▶ Acquire machines for the Administrative and Message Flow Servers. Optionally, you might need a machine for the AGPI Server as well.
 - Acquire new machine(s) or upgrade existing machine to meet your minimum hardware requirements.
 - Plan for physical disk. Calculate amount of disk storage you need initially and plan for upgrade and how additional disk is installed.

Note: The Administrative Server has the following minimum hardware requirements:

- ▶ Processor: an IBM xSeries® and Intel®-based dual processor system (or equivalent) with a minimum processor speed of 2.4 GHz
- ▶ Minimum memory requirements: 4 GB
- ▶ Minimum DASD requirement: 144 GB
- For high availability:
 - (1) Mirrored 36 GB boot disk
 - (1) Mirrored 3 x 36 GB shared disk
- ▶ Additional high-availability hardware requirements:
 - Microsoft certified cluster machine
 - Shared disk subsystem with RAID

Note: The Message Flow Server has the following minimum hardware requirements:

- ▶ Processor: an IBM xSeries and Intel-based dual processor system (or equivalent) with a minimum processor speed of 2.4 GHz
- ▶ Minimum memory requirements: 4 GB
- ▶ Minimum DASD requirement: 144 GB
- For high availability:
 - (1) Mirrored 36 GB boot disk
 - (1) Mirrored 3 x 36 GB shared disk
- ▶ Additional high-availability hardware requirements:
 - Microsoft certified cluster machine
 - Shared disk subsystem with RAID

After you finish

After you complete the tasks, you need to:

- ▶ Record the location and the physical information about the servers.
- ▶ Record disks that were added and how those disks are partitioned.
- ▶ Identify the upgrade path for disks for future disk storage needs.

Gateway

Unlike the hub which is centralized, Gateways are installed at each subscriber and publisher. A clean and secure physical space is required at each and every location for the Gateway. The hardware considerations and planning for Gateways are similar to that of the servers in the hub.

Before you begin

Before you begin, you need to:

- ▶ Create a list of possible locations where to deploy the Gateways.
- ▶ If you plan to use an existing machine, identify the machine and gather its current configuration.
- ▶ If you plan to acquire new machine, specify the minimum configuration.
- ▶ Record available disk storage.

Gateway hardware tasks

The Gateway hardware tasks include the following:

- ▶ Plan for physical site
 - Create a step-by-step process to ensure that you have a safe and secure physical site for the Gateway.
 - Make sure that you have the correct cabling.
- ▶ Acquire machines for the Gateway
 - Acquire new machine (or machines) or upgrade existing machine (or machines) to meet the minimum hardware requirements.
 - Plan for physical disk. Calculate the amount of disk storage that you need initially and plan for the upgrade and how additional disks are installed.

Note: The Gateway has the following minimum hardware requirements:

- ▶ Processor: an IBM xSeries and Intel-based dual processor system (or equivalent) with a minimum processor speed of 2.4 GHz
- ▶ Minimum memory requirements: 2 GB
- ▶ Minimum DASD requirement: 108 GB

After you finish

After you complete the tasks, you need to:

- ▶ Record the location and the physical information of the Gateway.
- ▶ Record the disks that were added and how those disks are partitioned.
- ▶ Identify the upgrade path for disks for future disk storage needs.

2.2.4 Planning for networking

The network infrastructure is essential for the secure exchange of clinical data in HCN and plays a critical role in the overall solution. Networking in HCN can be divided into two primary components, the network infrastructure and the network connectivity for the exchange of data. The network infrastructure include the network hardware devices and topology created with the interrelation between the hardware devices. The network connectivity relate to the network applications, host names and IP addresses. Connectivity also includes the network security which secures the network and the data transmitted from outside intruders as well as the management of the network.

Most HCN solution deployment scenarios already have network infrastructure in place, so our planning for networking will not consider the scenario where there is no network infrastructure. Planning for HCN networking focuses more on the connectivity, planning for the software, security and secure access.

Planning for network software

The network software planning identifies the HCN components and prerequisite software that require network resources as the first step towards creating the network software plan.

Before you begin

Before you begin, you need to:

- ▶ Create a list of all the HCN components and prerequisite software applications that require network resource.
- ▶ Create a list of the specific ports that HCN components and prerequisite software applications use.

Network software planning tasks

The network software planning tasks include the following:

- ▶ Obtain IP addresses for each server. Most networks establish a simple policy of assigning dynamic IP addresses to workstations and static address to servers. You should consider using static IP addresses for HCN servers and Gateways.
- ▶ Verify that the ports that HCN components and prerequisite software applications require exist and are not being used.
- ▶ Devise a naming scheme for all servers and Gateways.

After you finish

After you complete the tasks, you need to record all server and Gateway names and IP addresses.

Planning for network security

Your network security is perhaps the most critical aspect of your network planning. You must ensure that legitimate traffic get access while keeping out illegitimate attempts.

Before you begin

Before you begin the installation, you need to:

- ▶ Record all network entry points to your HCN network.
- ▶ Revisit your corporate network security policy and ensure that it does meet the HCN security and privacy requirements for transmission of clinical data.

Network security planning tasks

The network security planning tasks are as follows:

- ▶ Create firewalls. Firewalls should already be an integral part of your corporate security policy. You should place the HCN hub and Gateways behind your firewalls. You should only open ports that are required for HCN but were not already open in your firewall and limit the traffic to HCN only.
- ▶ Plan for virus and spyware protection. Malware are viruses and other harmful software that disguise as legitimate data or content to gain access to your network to perform malicious activities. It is expected that your corporate network policy already calls for use of antivirus and antispyware applications with frequent updates.

After you finish

After you complete the tasks, you need to:

- ▶ Record your network security policy changes including those to your firewalls.
- ▶ Record the list of antivirus and antispyware applications that you installed.

2.2.5 Planning for data interoperability

The Healthcare industry uses a wide variety of standard and nonstandard terminologies. Many healthcare organizations routinely access information from various hospitals, billing agencies, and so on. These entities might or might not have data in the same format. Currently, only a few organizations share a common standard vocabulary. For example, Hospital 1 might refer to a heart attack as an *acute myocardial infarction*, a research lab might refer to a heart attack as an *AMI*, and Hospital 2 might refer to the a heart attack as *congestive heart failure*. In many countries, there are massive efforts toward standardization using common terminologies. Standard vocabulary provides a common platform, and ensures all the entities speak the same language.

When beginning a healthcare collaboration effort, it is important to understand the terminologies used in the electronic data. For example, most hospitals to date do not capture symptoms and patient history in electronic form. If they do, it is probably not coded using LOINC. The HCN Gateway does have the capability of mapping observations coded in a local/nonstandard vocabulary into LOINC. Currently the HCN supports HL7 version 2.x and LOINC vocabularies. It has the capability to handle other vocabularies, however this needs customization. Careful assessment of the formats of the data and time for integration should be assessed as this could sometimes get complicated.

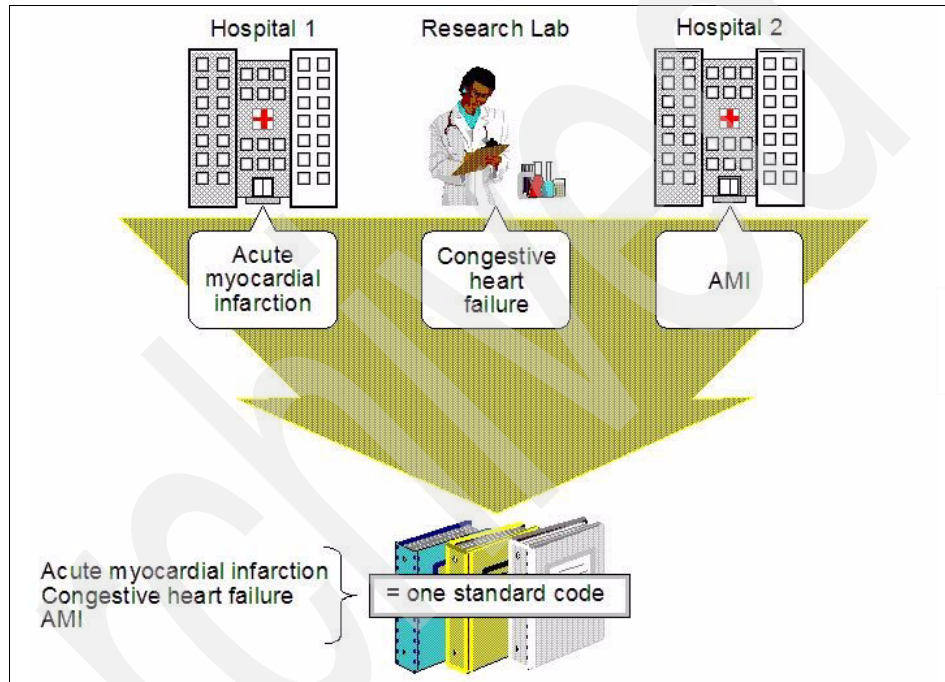


Figure 2-4 Data interoperability

Before you begin

Before you begin, you need to:

- ▶ Determine what healthcare domains (for example, pharmacy, laboratory, microbiology, symptoms and vital signs) are of interest to Data Review Organizations in your HCN network and what domains are likely to be of interest in the future.
- ▶ Determine what standard and nonstandard healthcare terminologies are used by all collaborating organizations in your network, and what terminologies are likely to be used in the future.

- ▶ Work with all participants to select the appropriate terminology to use in each identified healthcare domain. Choosing a standardized terminology will have many advantages; however, if nonstandard terminologies are widely used by many participants, these can be chosen for practical reasons.
- ▶ Determine where mapping between various terminologies will occur. If the terminologies are used in the HCN Clinical Topics to select data to be sent to the Data Review Organizations, the mapping must occur in the HCN Publisher Gateway. If the data is of interest to Data Review Organizations but not used to select messages for publication, the mapping could occur in the HCN Subscriber Gateway or in the IT systems of the Data Review Organization.
- ▶ Identify subject matter experts in each organization and in each healthcare domain who will perform the mappings or assist an IT specialist in performing the mapping.

Data interoperability planning tasks

The data interoperability planning tasks include the following:

- ▶ Leverage subject matter expertise to build the terminology maps in some implementation-neutral tool (such as a spreadsheet).
- ▶ Implement the mappings in the selected terminology (for example, Python scripts in the HCN Publisher Gateway, or SQL in the Data Review Organization's database). Note that some mappings are not one-to-one and might require more complex algorithms to determine the accurate term in the target vocabulary.

After you finish

After you complete the tasks, you need to:

- ▶ Have the mappings reviewed by additional subject matter experts to ensure clinical accuracy.
- ▶ Retain the implementation-neutral representation of the maps for future reference
- ▶ Put a process in place to review the terminology maps periodically as new terms are added to either the source or target vocabularies

2.2.6 Planning for capacity and performance

The performance and capacity of HCN can be greatly improved by modifying the physical infrastructure (that is, the hardware and network infrastructure) and by re-configuring the application and system software (that is, the operating system, the prerequisite software and the HCN components).

For information about how to tune the Gateway, WebSphere Business Integration Server, the Message Flow Server and DB2 databases to further enhance message processing and throughput in HCN, see AppendixC, “Performance tuning” on page 235. This section walks through scenarios to improve performance as applicable within the scope of this redbook.

Effective planning ensures that you can balance the various options to attain the optimal processing performance in your HCN implementation.

Before you begin

Before you begin, you need to record the following:

- ▶ Your network and servers (hardware) configuration.
- ▶ Your system design for the Message Flow Server and Publisher Gateways.
- ▶ The usage pattern at the publishing organizations. For example the pattern for entering medication orders into the pharmacy system at the end of rounds in a hospital ward will generate bursts of entries for processing at the HCN Publishing Gateway. By identifying these patterns, you will be able to tune the Publisher Gateway appropriately to process the entries efficiently.
- ▶ The current performance, capacity and throughput of your HCN installation.
- ▶ Current size of your databases.

Capacity and performance planning tasks

The capacity and performance planning tasks include the following:

- ▶ Refer to AppendixC, “Performance tuning” on page 235 for detailed steps about how to tune HCN for performance and throughput improvement.
- ▶ Project expected rate of publication.
- ▶ Project expected rate of growth of data.
- ▶ Plan for capacity upgrade.

After you finish

After you complete the tasks, you need to:

- ▶ Record the new performance, capacity and throughput of your HCN installation.
- ▶ Monitor rate of growth of publication and data.

2.2.7 Planning for privacy and security

Secure processing and transmission of medical information, coupled with protection of personal data are essential for all HCN publications.

Implementation of security and privacy in HCN were based on classes for the protection of patient information:

- ▶ Confidentiality. The protection of information so that unauthorized people, resources, and processes cannot access it.
- ▶ Integrity. The protection of information from unauthorized changes.
- ▶ Authentication. The protection of access to patient information by ensuring that users who access information are who they claim to be.
- ▶ Non-repudiation. The protection that sources of information cannot later deny having sent it.

Attaining the highest levels of security and privacy require taking critical steps to achieve confidentiality, integrity, authentication and non-repudiation. It should also include the institution of appropriate processes to ensure proper execution. Implanting all this does require elaborate planning. The following are some of the considerations that will enable you to plan for security and privacy for your HCN deployment.

Before you begin

Before you begin, you need to record any government legislation and mandates for protecting and securing medical information.

Privacy and security planning tasks

The privacy and security planning tasks include the following:

- ▶ Create the legal contract which organization's wishing to join the network must sign. The agreement must spell out the security and privacy standards and policy. The security and privacy policies must conform to all laws and mandates for processing medical information.
- ▶ Record the range of topics you publish and establish the privacy level(s) for each topic.
- ▶ Create process and criteria for approving subscription requests and assigning privacy levels.
- ▶ Create process and criteria for adding new users to your HCN and assigning them to gateways and hence privacy levels.
- ▶ HCN allows self signed certificates for Secure Sockets Layer (SSL), you have to consider if you need to obtain certificates from a recognized certificate authority such as Verisign.

Note: Refer to Chapter 6, "Privacy and security" on page 165 for more information about the implementation of privacy and security in HCN.

After you finish

After you complete the tasks, you need to put a process in place to review your security and privacy policy periodically.

2.2.8 Planning for service and support

The first step in having a successful HCN solution is to follow carefully the guidelines for installing and configuring the HCN prerequisite software and the HCN components. After you have it up and running, you have to keep it running to go on enjoying the real-time messaging and dissemination of clinical data. To do that, you do need a service and support plan. A successful service and support plan ensures that you get the latest updates to the HCN components, prerequisite software, and the Windows operating system. It ensures that you receive support for IBM software and hardware so that your HCN solution continues to operate uninterrupted. The service should customize and enhance your HCN solution to ensure that it meets your unique requirements.

IBM offers a plethora of services ranging from planning, design, installation, and implementation to managing your IT environment. It provides onsite and remote support options which enable you to choose the services that suit your needs and when you need them. IBM service support is designed to protect your IT investment, integrate new technologies into your HCN solution environment, and give you access to the support you need to use your HCN productively.

Choosing the right services and support for your organization and solution scenario requires careful consideration. In this section, we will present topics for consideration to enable you to create a comprehensive plan for HCN service and support.

Before you start

Before you begin, you need to:

- ▶ Create a list of all support and service agreements you currently have.
- ▶ Record your organization's service and support process.
- ▶ Record the level of support you currently provide within your organization.
- ▶ Identify IBM service offerings and requirements.

Service and support planning tasks

The service and support planning tasks include the following:

- ▶ Select from the list of services available from IBM, including installation, implementation, maintenance, migration, support, relocation, data center, site enablement, site planning, and software.
- ▶ Identify the support and maintenance levels you need.

- ▶ Choose the support delivery method for the selected services (that is, remote or onsite support).

After you finish

After you complete the tasks, you need to:

- ▶ Record information and levels of your chosen services and support.
- ▶ Integrate the new support and services into your organization's service and support process.

2.3 Chapter summary

This chapter discussed the three stages for deploying HCN solutions and identified the items that you need to consider in order to create a comprehensive project plan for successful HCN deployment. The stages include preinstallation, installation, and postinstallation stages.

The second part of the chapter introduced sub-plans that are modular in nature and that identify the different topics that you need to consider to identify the activities for the sub-plan. The sub-plans include planning for education, software, hardware, networking, data interoperability, capacity and performance, privacy and security, and for service and support.

Installing and configuring IBM WebSphere Business Integration for HCN

This chapter discusses the steps to install and configure IBM WebSphere Business Integration for Healthcare Collaborative Network. It looks at the order for installing the HCN components to ensure that the solution is set up properly. This chapter also presents useful tips for identifying and resolving common installation errors as well as tips for validating your HCN solution.

This chapter includes the following sections:

- ▶ Solution installation overview
- ▶ Installation requirements and prerequisites
- ▶ Installing the Healthcare Collaborative Network hub
- ▶ Installing the Healthcare Collaborative Network gateway
- ▶ Configuring HCN security features
- ▶ Validating the installation
- ▶ Chapter summary

3.1 Solution installation overview

This chapter does not provide a detailed step-by-step installation and configuration guide. Rather, it highlights the most critical procedures to install, configure, and validate WebSphere Business Integration for Healthcare Collaborative Network (HCN) successfully.

For comprehensive installation and configuration procedures, use this chapter in conjunction with the solution documentation that is available at:

<http://publib.boulder.ibm.com/infocenter/imshelp/v3r0/index.jsp?topic=/com.ibm.hcn.doc/hcn.html>

Important: To install HCN successfully, ensure that you follow the installation and configuration steps carefully as documented in the *Installation and Configuration Guide* that is provided with the solution documentation.

3.2 Installation requirements and prerequisites

This section describes the sequence of activities that you must follow to install and configure the HCN main components successfully.

Before you can install HCN, you should ensure that your system meets the hardware requirements and that you have the necessary prerequisite software. The sections that follow list the requirements and prerequisites for each HCN component.

Important: Your installation process *must* follow the sequence of steps in the exact order that is listed here to ensure proper installation of the HCN solution:

1. Install the prerequisite software for the Message flow server.
2. Install the Message flow server.
3. Install the prerequisite software for the Administrative server.
4. Install the Administrative server.
5. Use the Administrative server to create the Gateway_IDs that are needed for the installation of the Gateways.
6. Install the prerequisite software for each Gateway.
7. Install the Gateways (Publisher, Subscriber or both).
8. Install the AGPI server (optional).

3.2.1 Hardware requirements

From an infrastructure perspective, you must install the Message flow server, the Administrative server, and the Gateways on separate machines. With the AGPI server, you have the option either to install it or not, and where to install it. You can install it on the same machine as the Administrative server or any other machine in your infrastructure.

Message Flow server

The minimum requirements for the Message Flow server are:

- ▶ Processor: an IBM xSeries and Intel-based dual processor system (or equivalent) with a minimum processor speed of 2.4 GHz
- ▶ Minimum memory requirements: 4 GB
- ▶ Minimum DASD requirement: 144 GB

For high availability:

- (1) Mirrored 36 GB boot disk
- (1) Mirrored 3 x 36 GB shared disk

Additional high-availability hardware requirements:

- Microsoft certified cluster machine
- Shared disk subsystem with RAID

Administrative server

The minimum requirements for the Administrative server are:

- ▶ Processor: an IBM xSeries and Intel-based dual processor system (or equivalent) with a minimum processor speed of 2.4 GHz
- ▶ Minimum memory requirements: 4 GB
- ▶ Minimum DASD requirement: 144 GB

For high availability:

- (1) Mirrored 36 GB boot disk
- (1) Mirrored 3 x 36 GB shared disk

Additional high-availability hardware requirements:

- Microsoft certified cluster machine
- Shared disk subsystem with RAID

HCN Gateway

The minimum requirements for the Gateway are:

- ▶ Processor: an IBM xSeries and Intel-based dual processor system (or equivalent) with a minimum processor speed of 2.4 GHz
- ▶ Minimum memory requirements: 2 GB
- ▶ Minimum DASD requirements: 108 GB

For high availability:

- (1) Mirrored 18 GB boot disk
- (1) Mirrored 2 x 36 GB shared disk

Additional high-availability hardware requirements:

- Microsoft certified cluster machine
- Shared disk subsystem with RAID

3.2.2 Software prerequisites

The HCN components (administration server, message flow server, the AGPI server and the gateways) were built using a number of IBM and non-IBM applications. These applications form the set of prerequisite software that you must install and configure appropriately before you can proceed with the installation of each HCN solution component. You must also ensure that you have not only the correct version of each application but also the right fix pack level for your solution to operate appropriately.

Note: In general, fix pack levels indicated are the minimum required fix pack level. Later fix packs will work. However, for IBM WebSphere MQ Series, only Fix Pack 7 can be used, due to an incompatibility between later fix packs and IBM WebSphere Business Integration Server Express.

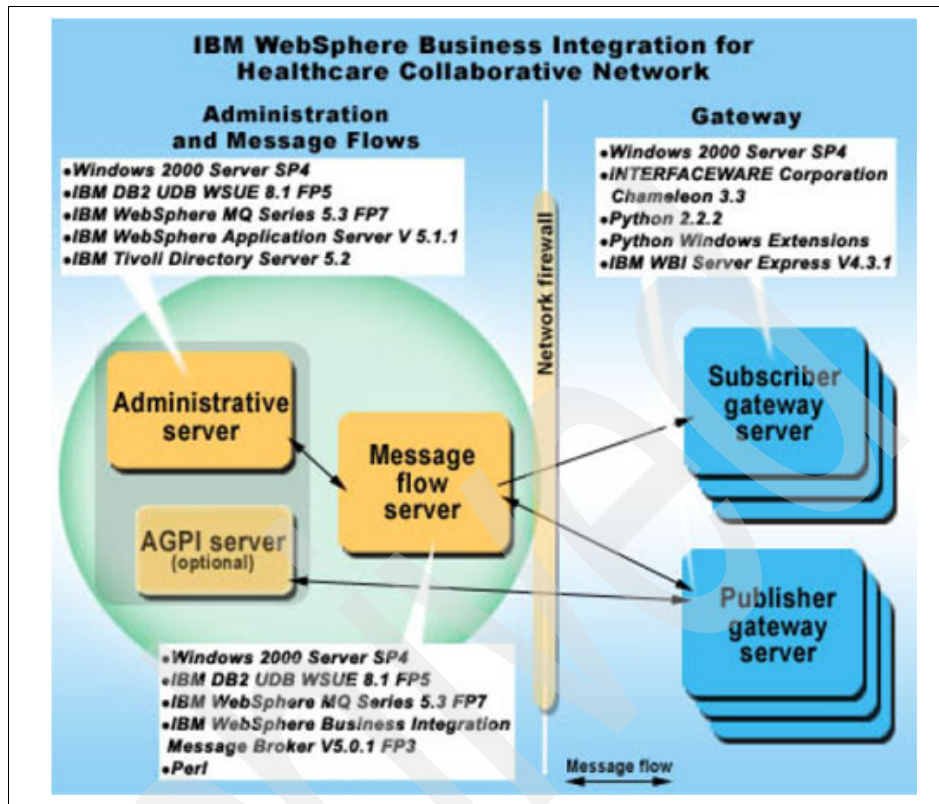


Figure 3-1 HCN components prerequisite software

Message flow server

Note: You *must* install the prerequisite applications in the order that we list them in this section.

The Message flow server prerequisite software includes the following:

1. MS Windows 2000 Server with Service Pack 4 plus current security patches available from Microsoft
2. IBM DB2 Universal Database Workgroup Server Unlimited Edition V8.1 Fix Pack 5

Note: IBM DB2 Universal Database Enterprise Server Edition Version 8.1 can also be used for the message flow server. You must install the corresponding Fix Pack 5 for this version of DB2.

3. IBM WebSphere MQ 5.3 Fix Pack 7
4. IBM WebSphere Business Integration Message Broker for Windows XP/2000 V5.0.1 FixPack 3
5. ActiveState ActivePerl at:
<http://www.activestate.com/Products/ActivePerl/>

Administrative flow server

Note: You *must* install the prerequisite applications in the order that we list them in this section.

The Administrative flow server prerequisite software includes the following:

1. MS Windows 2000 Server with Service Pack 4 plus current security patches available from Microsoft
2. IBM DB2 Universal Database Workgroup Server Unlimited Edition V8.1 Fix Pack 5
3. IBM WebSphere MQ 5.3 Fix Pack 7
4. IBM WebSphere Application Server Base V5.1.1 Fix Pack 1. 5

Before you install WebSphere Application Server Fix Pack 1.5, make a note of the files that are included in the <Installation_Directory>\AppServer\Java directory.

Note: Installation of WebSphere Application Server for the Administrative server require that you to stop the WebSphere Application Server before launching the **updatewizard** program for the Fix Pack 1.5 application. If you do not stop the server, it causes the fix pack installation to fail as shown in Figure 3-2.

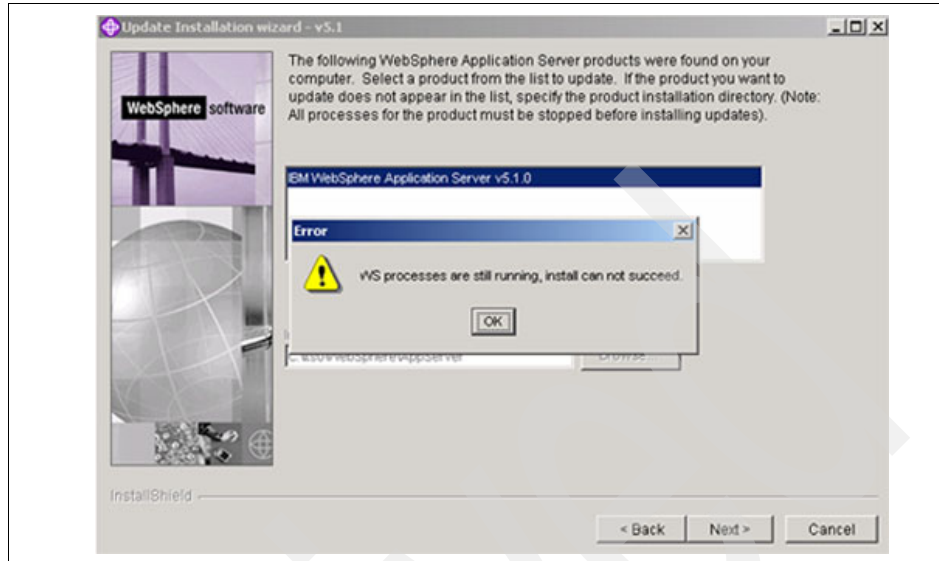


Figure 3-2 WebSphere Application Server update installation wizard failure

After installing the Fix Pack, verify that the files in the `<Installation_Directory>\AppServer\Java` directory were updated. It is essential that the updating of these files do take place. It is necessary to ensure that the creation of encrypted credentials for LDAP access are performed with the same version of the JCE archive (JAR file) included in the WebSphere Application Server Java libraries.

Example 3-1 shows an extract from the WebSphere Application Server SystemOut.log file, located in:

`<WAS_Installation_Directory>\WebSphere\AppServer\logs\server1`

The extract reports the error produced while unsuccessfully attempting to login into the WebSphere Application Server administration console. This is caused by an incorrect installation of the FixPack that did not update the above mentioned Java libraries.

Example 3-1 LDAP access exception

```
HCN Portal Logger - problem starting LDAP connection , Caused by
java.io.InvalidClassException: com.ibm.crypto.provider.1;
class invalid for deserialization
```

5. IBM Tivoli Directory Server 5.2

Note: Healthcare Collaborative Network Administrative server uses an SMTP server for e-mail notification purposes. In order to take advantage of this feature, you must install and configure on the Administrative server a SMTP server accessible at localhost:25.

AGPI server

You have the option of installing the AGPI server in your HCN solution or of making use of an AGPI service that is provided by a trusted party. If you choose to install an AGPI server, the supported approach is to install it on the same machine as the Administrative server, hence the software prerequisites for AGPI server are the same as that for Administrative server.

HCN Gateway

Note: You *must* install the prerequisite applications in the order that we list them in this section.

The HCN Gateway prerequisite software include the following:

1. Windows 2000 Server with Service Pack 4 plus current security patches available from Microsoft
2. INTERFACEWARE Corporation Chameleon 3.3 build 83 or later
3. Python 2.2.2 at:
<http://www.python.org/2.2.2/>
4. Python Windows Extensions (pywin32) build 202 at:
http://sourceforge.net/project/showfiles.php?group_id=78018
5. IBM WebSphere Business Integration Server Express V4.3.1 including the toolset. Required components in the IBM WebSphere Business Integration Server Express V4.3.1 bundle are as follows:
 - a. IBM WebSphere Business Integration Adapter for JDBC
 - b. IBM WebSphere Business Integration Adapter for JText
 - c. IBM WebSphere Business Integration Adapter for Web Services
 - d. IBM WebSphere Business Integration Adapter for WebSphere MQ
 - e. Java compiler SDK 1.3.1 (required for compiling custom maps and collaborations)
6. IBM WebSphere MQ 5.3 Fix Pack 7 (note that later versions of IBM WebSphere MQ Fix Packs are incompatible with WebSphere Business Integration Server Express)
7. IBM DB2 Universal Database Express Edition V8.1 Fix Pack 5

3.3 Installing the Healthcare Collaborative Network hub

Installing the HCN hub which includes the Message flow server, Administrative server and the optional AGPI server can only be performed after successful installation of the prerequisite software for each component.

The following checklists is a useful means for validating that the prerequisite software were properly installed. We also make use of the helpful information from installation log files for the prerequisite software validation process.

3.3.1 Message Flow server

The installation of the HCN Message flow server can only proceed after having successfully installed the prerequisite software and a positive review of the checklist in Table 3-1.

Table 3-1 HCN Message flow prerequisite software installation checklist

Prerequisite software	How to check	Expected value(s)
Windows 2000 Server SP4	From Windows command prompt type: winver	Version 5.0 (Build 2195: Service Pack 4)
IBM DB2 UDB Workgroup Server Unlimited Edition V.8.1 Fix Pack 5	From a DB2 command windows type: db2level	DB2 code release SQL08015 with informational tokens DB2 v8.1.5.449, s040212, WR21334, and Fix Pack 5
IBM WebSphere MQ 5.3 Fix Pack 7	From Windows command prompt type: mqver	Version: 530.7 CSD07 CMVC level: p530-07-L040527
IBM WebSphere Business Integration Message Broker for Windows XP/2000 V5.0.1 FixPak 3	From Windows command prompt type: regedit	Verify that the HKEY_LOCAL_MACHINE\SOFTWARE\IBM\WebSphereMQIntegrator\CurrentVersion shows: <ul style="list-style-type: none">► MQSeriesIntegratorVersion 5► MQSeriesIntegratorRelease 0.1► MQSeriesIntegratorUpdate 3
Perl	From Windows command prompt type: regedit	Verify that the HKEY_LOCAL_MACHINE\SOFTWARE\ActiveState contains the following folders: ActivePerl and PerlScript

For step-by-step instructions about how to install the HCN Message flow server, refer to the *IBM WebSphere Business Integration for Healthcare Collaborative Network - Installation and Configuration Guide*, which is available at:

<http://publib.boulder.ibm.com/infocenter/imshe1p1/v3r0/index.jsp?topic=/com.ibm.hcn.doc/hcn.html>

If no error conditions were encountered during the HCN Message flow server installation, the Message flow server log file `HcnMsgFlowInstallLog.txt`, which is located in the Message flow server installation directory should be error-free.

3.3.2 Administrative server

Before installing the Administrative server package it is recommended to check the versions of prerequisite software on the server. Table 3-2 show procedures for verifying the software version levels.

Table 3-2 HCN Administrative server prerequisite software installation checklist

Prerequisite software	How to check	Expected value(s)
Windows 2000 Server SP4	From Windows command prompt type: <code>winver</code>	Version 5.0 (Build 2195: Service Pack 4)
IBM DB2 UDB Workgroup Server Unlimited Edition V.8.1 Fix Pack 5	From a DB2 command windows type: <code>db2level</code>	DB2 code release SQL08015 with informational tokens DB2 v8.1.5.449, s040212, WR21334, and Fix Pack 5
IBM WebSphere MQ 5.3 Fix Pack 7	From Windows command prompt type: <code>mqver</code>	Version: 530.7 CSD07 CMVC level: p530-07-L040527
IBM WebSphere Application Server Base V5.1.1 Fix Pack 1.	Open the file <InstallDirectory>\WebSphere\AppServer\properties\version\BASE.product	<!DOCTYPE product SYSTEM "product.dtd"> <product name="IBM WebSphere Application Server"> <id>BASE</id> <version>5.1.1</version> <build-info date="06/27/2004" level="a0426.01"/> </product>
IBM Tivoli Directory Server 5.2	Locate the file <InstallDirectory>\IBM\HCN\LDAP\bin\level.txt	IBM Directory Release: aus52ldap Build: 031001a

For step-by-step instructions about how to install the HCN Administrative server, refer to the *IBM WebSphere Business Integration for Healthcare Collaborative Network - Installation and Configuration Guide*, which is available at:

<http://publib.boulder.ibm.com/infocenter/imshe1p1/v3r0/index.jsp?topic=/com.ibm.hcn.doc/hcn.html>

If no error conditions were encountered during the HCN Administrative server installation, the Administrative server log file `HcnAdminServerInstallLog.txt` which is located in the Administrative server installation directory should be error-free.

3.3.3 AGPI server

As mentioned in 3.3.3, “AGPI server” on page 73, if you choose to install the AGPI server, the supported and preferred approach is to install it on the same machine as the Administrative server. As such, the checklist for AGPI server installation is the same as that for Administrative server (see Table 3-2 on page 72).

For step-by-step instructions about how to install the AGPI server, refer to the *IBM WebSphere Business Integration for Healthcare Collaborative Network - Installation and Configuration Guide*, which is available at:

<http://publib.boulder.ibm.com/infocenter/imshe1p1/v3r0/index.jsp?topic=/com.ibm.hcn.doc/hcn.html>

If no error conditions were encountered during the HCN AGPI server installation, the AGPI server log file `HcnAgpiServerInstallLog.txt` which is located in the AGPI server installation directory should be error-free.

3.4 Installing the Healthcare Collaborative Network gateway

Before installing each Gateway, we recommend that you verify the versions of prerequisite software that are installed currently on each of your servers.

Table 3-3 shows the procedures for verifying the software version levels.

Table 3-3 HCN Gateway prerequisite software installation checklist

Prerequisite software	How to check	Expected value(s)
Windows 2000 Server SP4	From Windows command prompt type: winver	Version 5.0 (Build 2195: Service Pack 4)
iNTERFACEWARE Corporation Chamaleon 3.3 build 83 or later	Locate the file <InstallDirectory>\iNTERFACEWARE Chameleon\INSTALL.txt In Chameleon Toobar click: Help → About...	Verify that the file does not contain any installation error IDE Version 3.3 Engine Version 3.3 Engine Bulid Number: 83 (or higher)
Python 2.2.2 with Python Windows Extensions (pywin32) build 202	From a Windows command prompt type: python	Python 2.2.2 (#37, Oct 14 2002, 17:02:34) [MSC 32 bit (Intel)] on win32
IBM WebSphere Business Integration Server Express V4.3.1	Locate the file <InstallDirectory>\WebSphereServer\log\wbi_server_exp_install.log From Windows command prompt type: regedit	Verify that the file does not contain any exception. Verify that the HKEY_LOCAL_MACHINE\SOFTWARE\IBM\WebSphere Business Integration\Server Express currentVersion is set to 4.3.1
IBM DB2 UDB Universal Database ExpressV.8.1 Fix Pack 5	From a DB2 command windows type: db2level	DB2 code release SQL08015 with informational tokens“DB2 v8.1.5.449, s040212, WR21334, and Fix Pack 5
IBM WebSphere MQ 5.3 Fix Pack 7	From Windows command prompt type: mqver	Version: 530.7 CSD07 CMVC level: p530-07-L040527

Attention: Installing WebSphere MQ fix packs higher than Fix Pack 7 creates known issues with WebSphere Business Integration Server Express. You should only use the MQ CSD07.

For step-by-step instructions about how to install the HCN Gateway, refer to the *IBM WebSphere Business Integration for Healthcare Collaborative Network - Installation and Configuration Guide*, which is available at:

<http://publib.boulder.ibm.com/infocenter/imshe1p1/v3r0/index.jsp?topic=/com.ibm.hcn.doc/hcn.html>

Important: During the Gateway installation, the installation program prompts you to launch the WebSphere Business Integration Server. It is important that you launch the WebSphere Business Integration Server using the shortcut the installation program placed on the Desktop, and that you wait for up to one minute for the WebSphere Business Integration Server to complete initialization before selecting **OK**. Failure to do so results in the failure to deploy the HCN objects to the WebSphere Business Integration Server.

Also, during the installation, many command prompt windows open. It is important that you wait until these windows close automatically before moving to the next installation step. Interrupting the DOS processes causes the installation to fail.

In Chapter 2, “Planning and designing your HCN solution” on page 27, we discussed the importance of creating a project plan for your solution prior to embarking on the installation and configuration. Here, you find that the information from your solution planning and design is needed to complete the installation and configuration of Gateways. For proper Gateway configuration, the HCN administrator must perform the following steps:

1. From the Administrative console create entries for each organization joining the network and the primary user (and optionally additional users) for each organization.
2. Create Gateways for each organization and assign users and primary users to each Gateway.

Note: The assigned Gateways IDs and names will be used to properly configure the Gateways during the installation and configuration phases. The HCN Administration server converts Gateway names to all uppercase characters, so you must enter gateway names into the HCN Gateway installation program in uppercase

3. Enable the Gateways.

Note: Because this last operation sends e-mail notifications to the primary users of the organization to which the Gateway belongs, this step requires an SMTP server to be accessible from the HCN Administrative server.

Validating the Gateway server installation

The best way to validate the successful installation of your Gateways is by examining installation the following log files:

- ▶ *C:\Install directory\IBM\HCN\Configuration\config_logmddyyyy_xyzp.txt*
This file summarizes the key configuration parameters you selected during the installation process and shows the messages related to the creation and configuration of the MQ queue managers, queues and channels, and of the HCN Gateway database.
- ▶ *C:\Install directory\WebSphereServer\InterchangeSystem.log*
This file is the main log file of the WebSphere Interchange Server. It shows the messages related to the deployment of HCN Gateway connectors, collaborations, maps and business objects.

Starting the Gateway server

After a successful installation, you should be able start the Gateway server and connect to the underlying running WebSphere Business Integration Interchange Server through the System Manager by doing the following:

- ▶ Start the Gateway server.
To start the Gateway server, double-click the icon that was created during the installation on your Windows desktop named *Start Gateway Server*. A DOS command window opens. You must keep the window open while the Gateway is up and running.

Note: If the Gateway server does not start properly, be sure that the DB2 service is running. If not, start it manually from **Start → Settings → Control Panel → Administrative Tools → Services** or by running the **db2start** command from a DB2 command prompt.

- ▶ Connect to the WebSphere Business Integration Interchange server.
In order to connect to the WebSphere Business Integration Interchange server, on the Windows menu select **Start → Programs → IBM WebSphere Business Integration Express → Toolset Express → Administrative → System Manager** and right-click the existing Interchange server instance selecting **Connect** as shown in Figure 3-3.

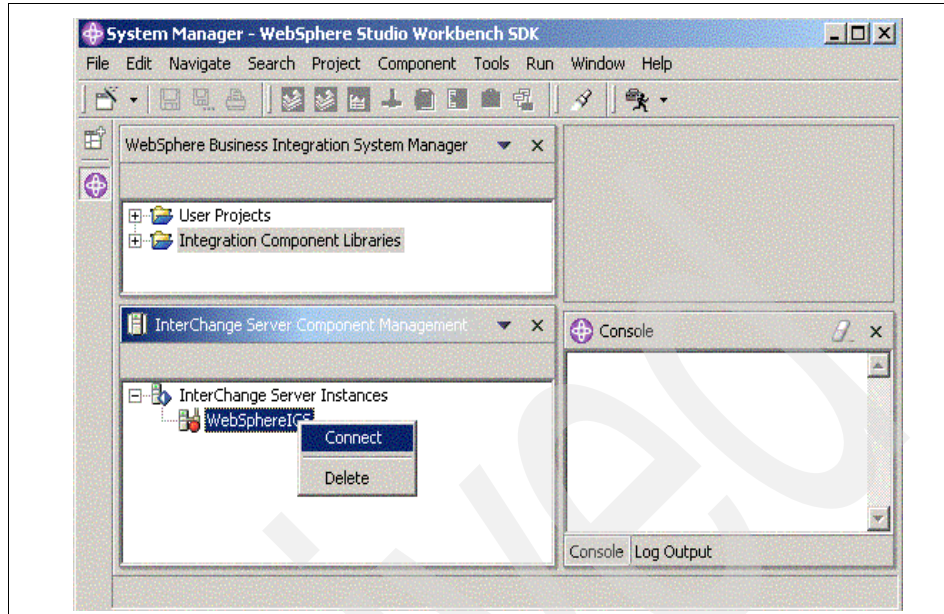


Figure 3-3 Connecting to the HCN Gateway server

- ▶ Log in as the default User
Logging in with the default User name admin and Password null you should be able to see the HCN specific objects: maps, collaboration, and business objects, connectors agent.
- ▶ Start Gateway collaborations
Make sure that all the Gateway collaborations objects, maps, and connectors agent are up and running. If not, right-click those that are paused or stopped or click the corresponding folder to restart them.

Note: You must start the Map *HCN_Publication_to_HCN_Message* manually.

3.4.1 Starting connector agents

Connectors in the IBM WebSphere Business Integration Server enable integration of various applications with HCN. Connectors consist of two logical parts, the connector controller and the connector agent. Connector agents interface directly with the applications being integrated (examples in HCN include databases, WebSphere MQ, and HL7 applications). The connector agent runs in a separate process which can run in the foreground, or be configured to run in

the background as a Windows service. In HCN, all connector agents are Java processes. During initial setup and testing phases, it is recommended that you run the connector agents in the foreground. If desired, you can configure the agents to run as services after you have verified the HCN configuration and tested the data exchange. See 5.3.2, “Running gateway components as Windows services” on page 152 for details.

The connector controller sends and receives data between the connector agent and the WebSphere Business Integration Server. The connector controller runs as one or more threads within the WebSphere Business Integration Server Java process.

The status of connector controllers and connector agents can be viewed through the System Manager. The status of connector controllers can be seen in the InterChange Server Component Management view by expanding the connectors folder and looking at the colored icons next to the connector name. The status of connector agents can be seen in the System View, in the column labelled *Agent Status*.

Not all of the connectors on an HCN Publisher Gateway need to be started. The following connectors must always be running for proper HCN Publisher Gateway operation:

- ▶ HCNBrokerConnector
- ▶ HCNPubDBConnector

HCN provides three connectors for receiving clinical data from applications: HCNHL7Connector, HCNEventFileConnector, and HCNEventQueue Connector. Without custom configuration, however, only two of these can be configured to connect to the WebSphere Business Integration Server at any given time; the default configuration connects the HCNHL7Connector and the HCNEventFileConnector. Only those connectors which are configured to connect to the WebSphere Business Integration Server must be started, so with the default configuration, the HCNEventQueue connector does not need to be started. This means that the HCNEventQueue connector controller can be stopped, and its connector agent does not need to be started.

For information about how to create additional connectors and the process for changing the default configuration to use other connectors, see “Creating additional connectors” on page 187.

The HCNAGPIConnector is only used when the AGPI server is present and being used in your HCN configuration. By default, the HCN Publisher Gateway is configured not to use an external AGPI server, but instead to generate anonymous patient IDs locally. When configured this way, the HCNAPGConnector does not need to be started.

With all desired connector controllers running you can then launch the connectors agents through the Desktop shortcuts automatically created during the Gateway installation. All the DOS processes that show logs of each controller will be executed in command prompt windows that must be kept open in order to allow the connectors to run.

Note: For correct startup of each connector, the WebSphere MQ channels and cluster queues must be running and visible from each Gateway. For details refer to the HCN solution *Installation and Configuration Guide* in the WebSphere MQ cluster configuration paragraph of the Message flow server section.

While the configuration of most connectors is automatic, when installing a Publisher gateway to use AGPI server, the AGPI connector must be manually configured in order start successfully. To do so, you are required to do the following:

1. Start the System Manager.
2. Connect to the Interchange server.
3. Right-click the Hospital_to_Gateway_AGPI collaboration.
4. Select the connector **Properties**.
5. Define the following variables to allow the Gateway to access the AGPI server:
 - AGPI_SERVER_USERID
 - AGPI_SERVER_PASSWORD
 - USER_EXTERNAL_AGPI_SERVER

You should define the values of these variables during the configuration of the AGPI server.

3.5 Configuring HCN security features

HCN makes use of Secure Sockets Layer (SSL) to ensure secure transmission of data over the Internet. This section provides practical information for enabling and correctly configuring SSL in HCN.

For a step-by-step guide on how to configure SSL for HCN, refer to the HCN *Installation and Configuration Guide* at:

<http://publib.boulder.ibm.com/infocenter/imshep1/v3r0/index.jsp?topic=/com.ibm.hcn.doc/hcn.html>

For details on SSL concepts and on security policies management within HCN you are encouraged to refer to Chapter 6, “Privacy and security” on page 165.

We start with the assumption that the following are in place:

- ▶ You configured a WebSphere MQ cluster topology while installing the prerequisite software products

During the installation process, different MQ clustering requirements have to be met to allow HCN to work properly. HCN uses this MQ feature to enable better management and administration, with a simplified topology. The clustering feature stores connectivity information — the topology of the cluster — in repositories that are owned and managed by MQ queue managers. Best practices recommend that you should create two full repositories in the cluster to allow for availability and redundancy (that is, a primary and a secondary repository). In HCN these two repositories are in the Message flow server and in the Administrative server, respectively.

For detailed information about how to install and configure WebSphere MQ cluster and on how to configure and enable SSL in the Administrative server's WebSphere Application Server refer to the HCN *Installation and Configuration Guide*.

- ▶ The WebSphere Application Server was appropriately deployed and configured for the Administrative server, and enabled for SSL to provide secure communication between the Internet web clients and the Administrative server portal application

To validate the WebSphere Application Server SSL configuration, connect to the Administrative server portal main page at:

`https://<Admin_Server_Name>/hcn/index.html`

If the WebSphere Application Server SSL is properly configured, a Security Alert opens, as shown in Figure 3-4.



Figure 3-4 Certificate security alert

If you select **Yes**, the HCN welcome page opens, as illustrated in Figure 3-5.

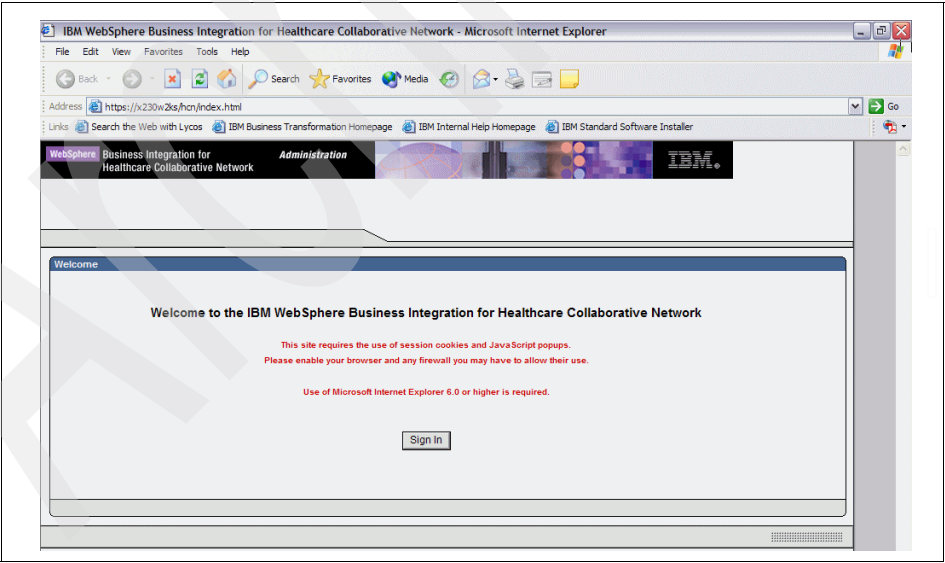


Figure 3-5 HCN welcome page

WebSphere MQ SSL requires the creation and management of certificates to provide secure connection channels among the various HCN components. To enable WebSphere MQ SSL, you must install and assign digital certificates to the communicating MQ queue managers associated with each HCN component. This means that any two HCN components communicating over an SSL enabled MQ channel must have unique certificates assigned to them and each must also locally store the other component's public certificate.

Digital certificates can be produced by a trusted third party, generally referred to as Certificate Authority. Alternatively, you can generate self-signed digital certificates through the system itself if no certificates from a Certificate Authority are available.

Your overall solution architecture should be taken into careful consideration while enabling SSL in HCN. For example, in a HCN cluster, the AGPI server exchanges data with Publisher gateways. For availability and redundancy reasons the cluster requires the AGPI server's public certificate to be stored in both the Message flow server (the primary cluster repository) and the Administrative server (the secondary cluster repository). Hence, the AGPI certificate was installed and assigned to the queue managers in the Administrative server, in the Message flow server, in the AGPI server itself and in the two Publisher gateways that are part of our scenario.

The following checklist summarizes the key steps to be performed before implementing the SSL on HCN:

1. Ensure that you have a certificate for each HCN server. You can create a self-signed certificate or obtain one from a Certificate Issuing Authority.
2. For each HCN component, import and assign its own certificate to the local queue manager. Then import and assign the public certificates for the other HCN servers as suggested in Table 3-4.

Table 3-4 Installing certificates on each HCN component

HCN component	HCN components' certificates
Administrative server	<ul style="list-style-type: none"> ▶ Administrative server (assign) ▶ AGPI server, if installed (import) ▶ Message flow server (import) ▶ Subscriber gateways (import) ▶ Publisher gateways (import)
Message flow server	<ul style="list-style-type: none"> ▶ Message flow server (assign) ▶ AGPI server, if installed (import) ▶ Administrative server (import) ▶ Subscriber gateways (import) ▶ Publisher gateways (import)

HCN component	HCN components' certificates
AGPI server, if installed	<ul style="list-style-type: none"> ▶ AGPI server (assign) ▶ Message flow server (import) ▶ Administrative server (import) ▶ Publisher gateways (import)
Subscriber gateways (each)	<ul style="list-style-type: none"> ▶ Subscriber gateway (assign its own certificate) ▶ Message flow server (import) ▶ Administrative server (import)
Publisher gateways (each)	<ul style="list-style-type: none"> ▶ Publisher gateway (assign its own certificate) ▶ Message flow server (import) ▶ Administrative server (import) ▶ AGPI server, if installed (import)

- For each HCN component, enable the SSL communication on each queue manager (Figure 3-6). This operation often requires each queue manager in the HCN cluster to be restarted in order to map all the certificates in the topology.

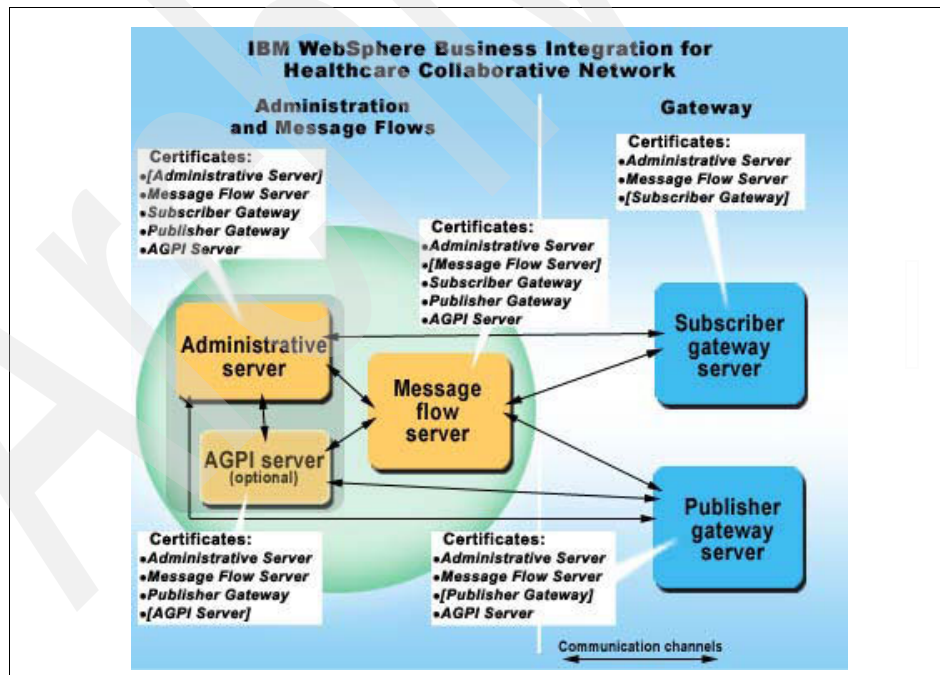


Figure 3-6 Certificates on each HCN component

Creating self-signed certificates

If you do not have digital certificate issued by a Certification Authority, the only way to implement SSL communication and encrypt the MQ channels between the various elements of HCN is to generate and install self-signed certificates. Together with the Administrative server prerequisite software, HCN provides the tool that you can be used to generate self-signed certificates. The tool is called *IKeyman*, and it is located in the following Administrative server directory:

C:\<Installation directory>\IBM\gsk7\bin

After starting the IBM Key Management application (gsk7ikm.exe) you should create key database files for each HCN component as specified in HCN *Installation and Configuration Guide*. Figure 3-7 shows the tool with an example of a key database file for the hospital publishing gateway in our scenario.

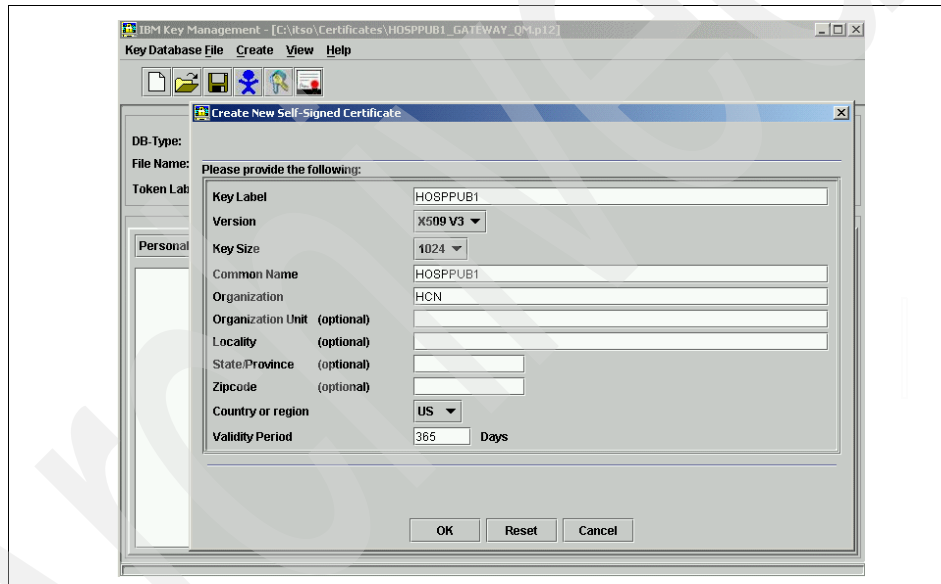


Figure 3-7 IKeyman tool: Creating hospital publisher gateway key database file

The key database file acts as a container where to store the real certificates that, as already mentioned can be self-signed or issued by a Certification Authority.

In our implementation, we use self-signed certificates by selecting **Personal Certificates** (Figure 3-8) and then clicking **New Self-Signed** (Figure 3-9) filling the key file properties.

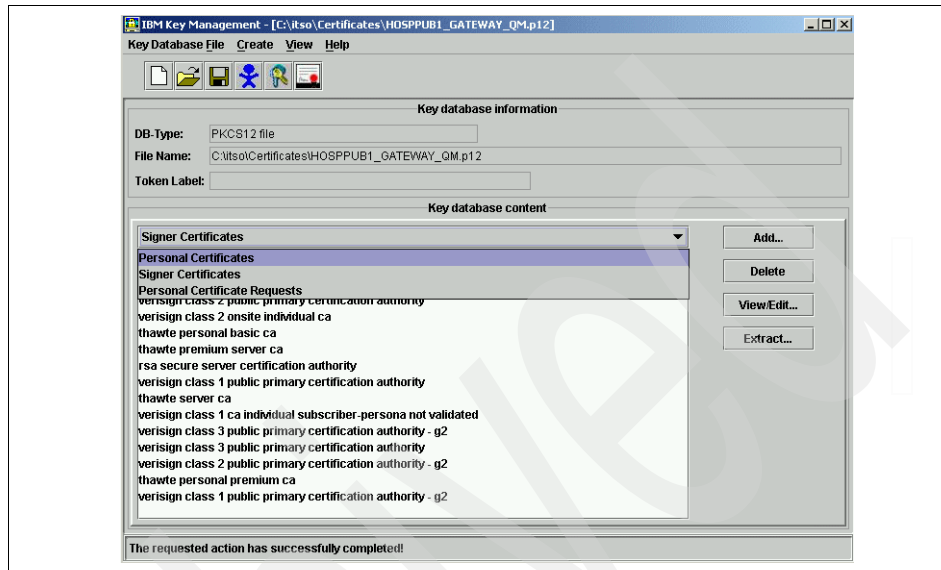


Figure 3-8 Key database content: Selecting Personal Certificates

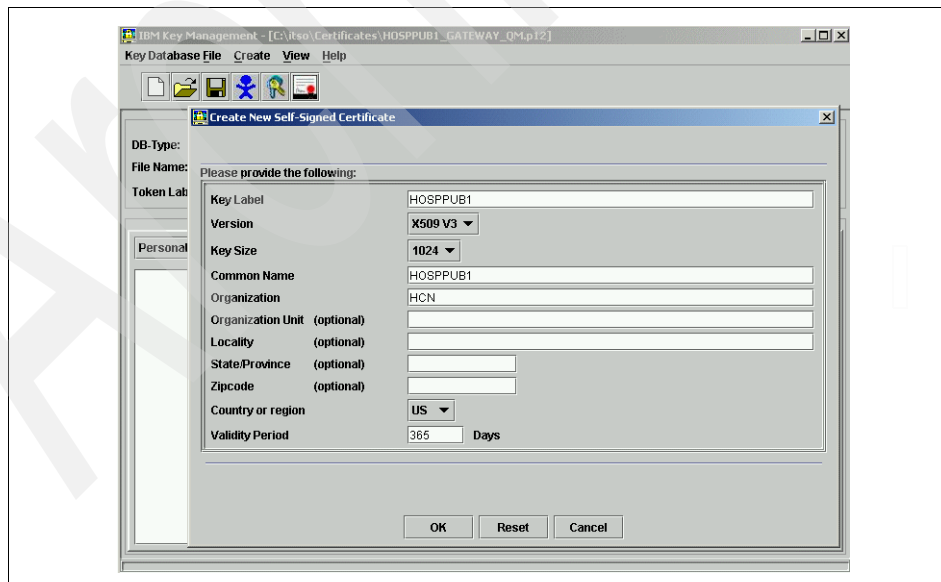


Figure 3-9 New self signed certificate properties

After creating self-signed certificates for each gateway, the Administrative server, the Message flow server and, if present, for the AGPI server, the certificate files can then be appropriately copied to any remote machines in your HCN solution, as stated in Table 3-4 on page 82.

Importing certificates and enabling SSL

Two steps are still required to have the SSL up and running into HCN:

1. On each server, import the certificates into the queue managers' key store

Start the MQ Explorer from Windows menu of the local machine **Start → Programs → IBM WebSphere MQ → WebSphere MQ Explorer**.

Then add and assign the appropriate certificates on the local queue manager according to Table 3-4. This operation often requires the cluster to be restarted in order to find all the certificates that have been added.

Tip: Before importing the certificate files on the various HCN machines check the operating systems' date consistency. In fact, if the date of the operating system of the machine on which you are adding the certificates is prior to the certificate's creation date, you can get the error shown in Figure 3-10.



Figure 3-10 SSL certificate date inconsistency error

2. On each server, enable WebSphere MQ SSL on any queue manager by setting the proper encryption algorithm on the communication channels.

After having imported the appropriate certificates and assigned a unique certificate to each queue manager, you should:

- a. Stop all the cluster channels on the queue managers before changing the encryption algorithm.

- b. Set the encryption algorithm for the cluster sender and cluster receiver channels according to your security policy. For example, according to the US HIPAA, the Triple DES encryption is among the compliant algorithms. In this case, select the **TRIPLE_DES_SHA_US** encryption.

3.6 Validating the installation

The final step in the installation and configuration of your HCN solution should be to validate that each element is indeed properly installed, configured and running. In particular all the Gateways, both Publishers and Subscribers, must have all the required connectors up and running. We use the Public Health Alert sample scenario we implemented in the course of writing this redbook to show you some key tests you can use to validate your solution.

Our Public Health Alert scenario includes one subscriber and two publisher gateways, in addition to the Message Flow and the Administrative/AGPI server. Figure 3-11 shows the physical layout for the Public Health Alert scenario. The AGPI server is installed on the same machine as the Administrative Server, which also hosts an FTP server for receiving publication logs from message flow server and an SMTP server for e-mail notifications (Note that you could use any existing SMTP server in your infrastructure).

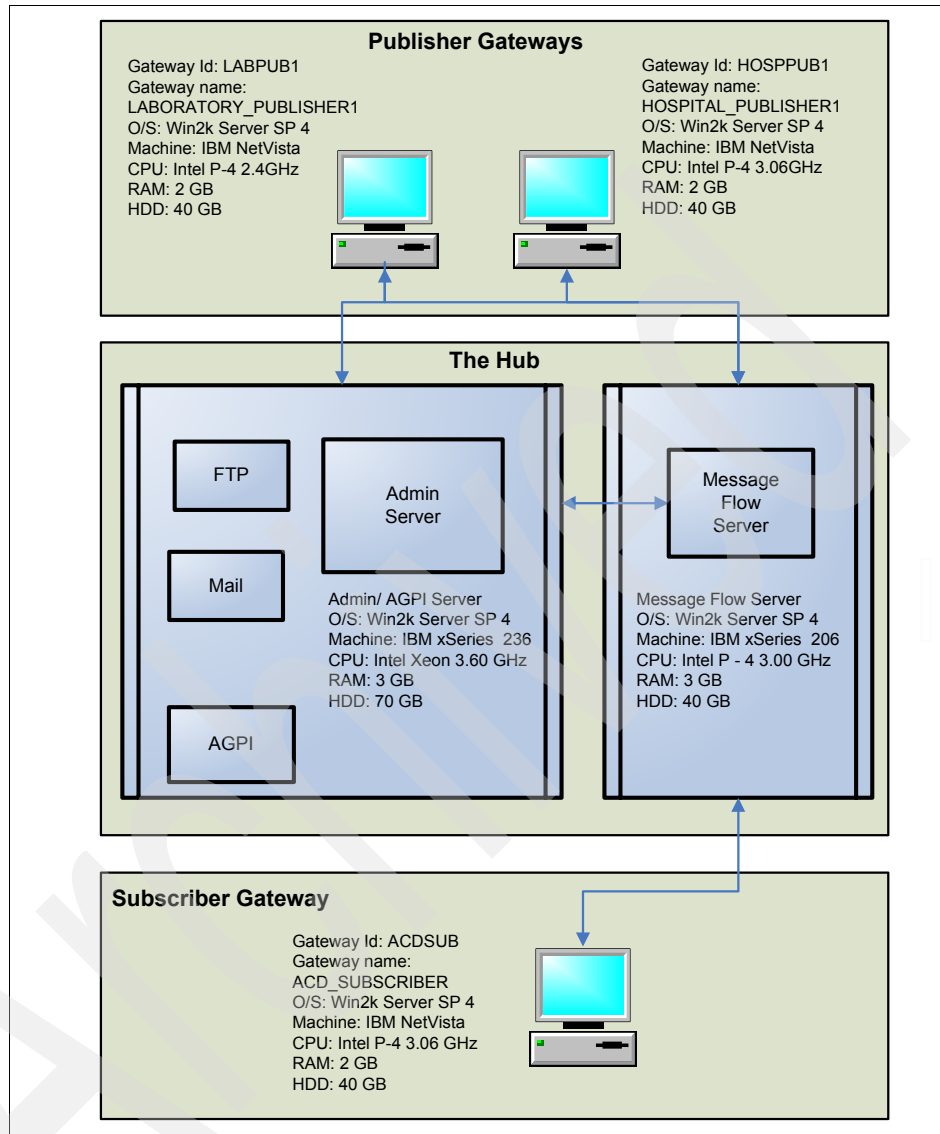


Figure 3-11 ITSO HCN Public Health Alert scenario physical layout

3.6.1 Validating the WebSphere MQ configuration

A good way to check the consistency of the whole solution is to start with the Gateways. On the WebSphere MQ Explorer console start by clicking on **Start** → **Programs** → **IBM WebSphere MQ** → **WebSphere MQ Explorer**. Then, follow these steps:

1. Select the local queue manager (its name is the name of the gateway concatenated with .MGQM).
2. Ensure that the **View** → **Show Cluster Queues** is selected.

You should see, besides the corresponding local queues, the following Message flow cluster queues:

- ▶ MQSI_INQ, the Publication queue

This queue receives messages to be published to the subscribers either in a form of e-mail notifications (through the Administrative server) or in a form of MQ messages on the subscriber queues.

- ▶ MQSI_INC, the Message flow server command queue

This queue receives command messages from the Administrative server for publications and subscriptions.

- ▶ MQSI_ING, the Gateway command queue

This queue receives command messages targeted to one of the Gateway servers that is identified by the publisher ID as part of the Gateway command message.

- ▶ MQSI_INR, the Gateway response queue

This queue receives response messages sent from the Gateway to the Administrative server as a response for a command.

- ▶ MQSI_ERR, the error notification queue

This queue receives error messages from one of the Gateways indicating an internal error happened while processing a message on the Gateway. This message is forwarded to the Administrative server to send e-mail to the administrator describing the error.

If Gateway installation and configuration have been successful, the Queues folder for the local queue manager should look similar to the one in Figure 3-12 on page 90.

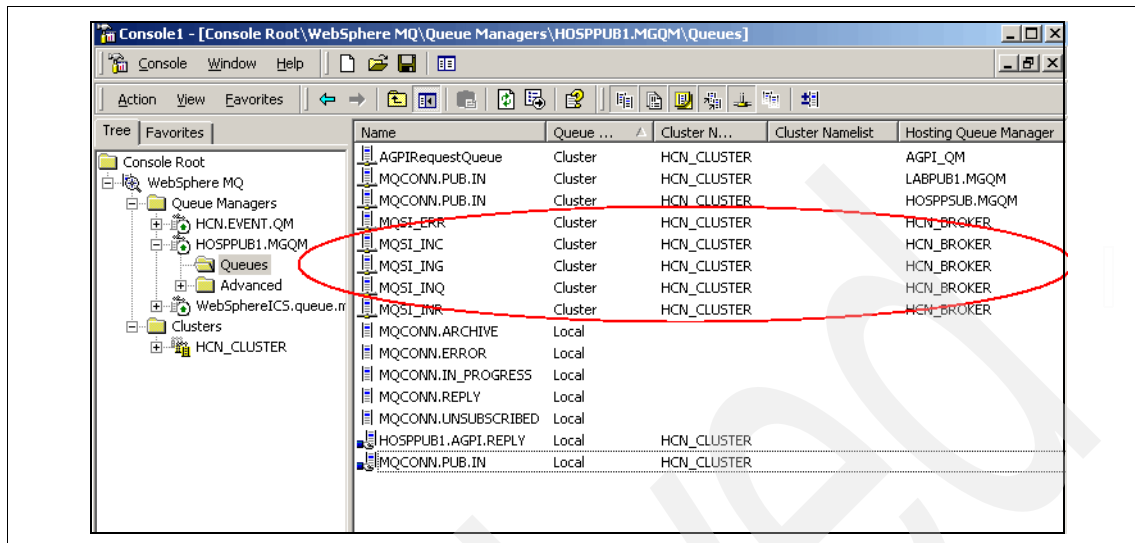


Figure 3-12 Publishing Gateway queues in the publishing hospital

The mechanism by which WebSphere MQ transmits information about the cluster configuration is asynchronous, and it can take several hours for the remote queues to show up in the MQ Explorer view. If, after waiting several hours or overnight, the cluster queues are still not visible from the Gateways, perform the following operations:

1. Ensure that the channels that are associated with the Gateway's local queue manager are running.
 - a. In WebSphere MQ Explorer console click the Channels folder located in the Advanced directory that is associated to the local queue manager.
 - b. Each Gateway should show three channels, the service CHANNEL1, Cluster sender, and Cluster receiver (see Figure 3-13 on page 91). All these three must be in the running state. Note that an inactive state does not necessarily indicate an error; continue with the following if one or more of the channels shows inactive.

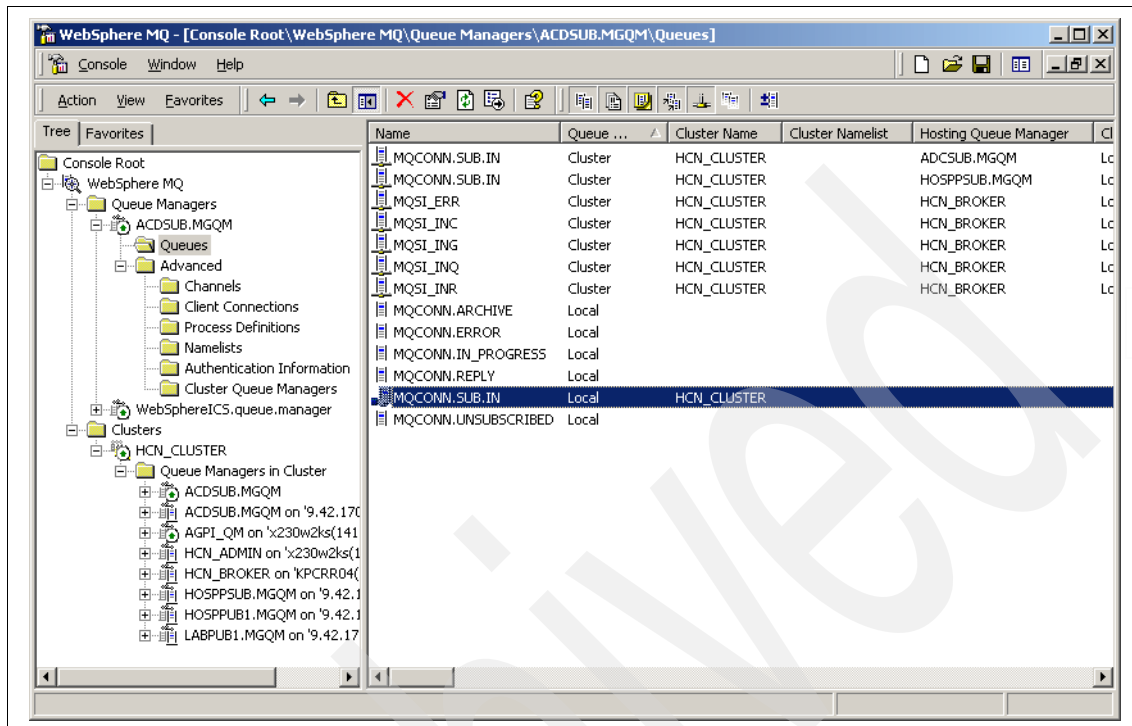


Figure 3-13 Channels in the publishing Hospital WebSphere MQ Explorer console.

2. If the channels are not running, refer to the WebSphere MQ cluster configuration paragraph of the Message flow server section in the HCN *Installation and Configuration Guide*. (See 5.4.1, “WebSphere MQ queues and Queue Managers” on page 159 for tips on troubleshooting WebSphere MQ in HCN.)
3. If the channels are running but the cluster queues are still not visible, we recommend that you force input data into each cluster queue manually using the MQ command **amqsput** from the Gateway Windows command prompt as follows:

```
amqsput Cluster_queue_name GATEWAY_LOCAL_QUEUE_MANAGER
```

If the **amqsput** command does not display an error message, it will display a blank line and begin accepting input. You should press Ctrl+Z, then press Enter, to terminate the **amqsput** command avoid placing an invalid message on the queue.

After refreshing the queue list in WebSphere MQ Explorer console you should be able to see all the cluster queues. Figure 3-14 on page 92 illustrates the Queues

folder for the ACD Institution (from our Public Health Alert scenario) that implements a Subscriber Gateway

MSGID	OBSERVATIONID	SUBID	CODINGSYSTEM	DESCRIPTION
0	100-8	OBSUBID	CODESYS	DESC
1	100-8	OBSUBID	CODESYS	DESC
2	100-8	OBSUBID	CODESYS	DESC
3	100-8	OBSUBID	CODESYS	DESC
4	100-8	OBSUBID	CODESYS	DESC
5	100-8	OBSUBID	CODESYS	DESC
6	100-8	OBSUBID	CODESYS	DESC
7	100-8	OBSUBID	CODESYS	DESC
8	100-8	OBSUBID	CODESYS	DESC
9	100-8	OBSUBID	CODESYS	DESC
10	100-8	OBSUBID	CODESYS	DESC
11	100-8	OBSUBID	CODESYS	DESC
12	17012-6	OBSUBID	LOINC	INFLUENZA A AB

Figure 3-14 Subscriber Gateway queues in the ACD institution.

3.6.2 Validating HCN data flow

The essential step for validating a complete HCN installation is to check the information flow among its various components. In our Public Health Alert scenario, we tested the installation by sending test messages from the two Publishing Gateways into the network.

Even if no error were detected during the installation process, you still need to verify the basic functions of HCN:

- ▶ That correct messages are sent
- ▶ That the subscriber database tables have been updated
- ▶ That the subscriber is notified of the new publications

For further details on users, organizations, notifications, topics and on how to perform each of the following tasks, refer to Chapter 4, “HCN entities and functional components” on page 97. The following lists the sequence of steps that you must execute to test the correctness of the integration and configuration of the whole HCN solution:

1. Log into the portal as HCN administrator.
2. Create organizations.
3. Create primary users for each organization and each gateway, ensuring that each of them has an active and valid e-mail address.
4. Create publishers, subscriber and observer users, ensuring that each of them has an active and valid e-mail address.
5. Create and enable logical gateways.
6. Associate organizations with the correct users and gateways.
7. Log in as a subscriber user.
8. Create a Public Health Alert topic and subscribe to it selecting information transmission in both e-mail and data format. The reason is to verify flows in both MQ queues and e-mails.
9. Log in as a publisher user.
10. Verify the request for publications on the selected topic and create a corresponding new publication.
11. In the corresponding publisher gateway store an HL7 message representing the new publication in the following directory:
`<InstallationDirectory>\HCN\Gateway\Publisher Gateway\Runtime\in`
12. After a while (up to 2 minutes with the default polling intervals), the polling mechanisms triggers the HCN flow and you should be able to see in the subscriber's e-mail account a message similar to that shown in Example 3-2 that notifies you that a new publication that matches the requested topic has been submitted.

Example 3-2 An example of HCN notification sent by e-mail to subscribers

From: <admin@hcn.itso.ibm.com>
To: <drlakshmi@itsoacd.gov>
Sent: Saturday, September 10, 2005 5:28 PM
Subject: HCN Notification - Topic 'Influenza_A_H5N1_reports' has been matched

Rule triggered for topic 'Influenza_A_H5N1_reports' at
'HOSPITAL_PUBLISHER1' on '2005-09-10T18:35:11-04:00' for patient
'AGPI-000000000224'.

This message has been automatically generated. Do not reply to it.

If you have any questions or concerns, please contact the HCN administrator at admin@hcn.itso.ibm.com.

13. The next step is to verify that the HL7 message has been sent to the subscriber gateway. Follow these steps:
 - a. Open the MQ Explorer on the subscriber gateway through Windows menu **Start** → **Programs** → **IBM WebSphere MQ** → **WebSphere MQ Explorer**.
 - b. Open the **Queue Managers** folder and select the local gateway queue manager.

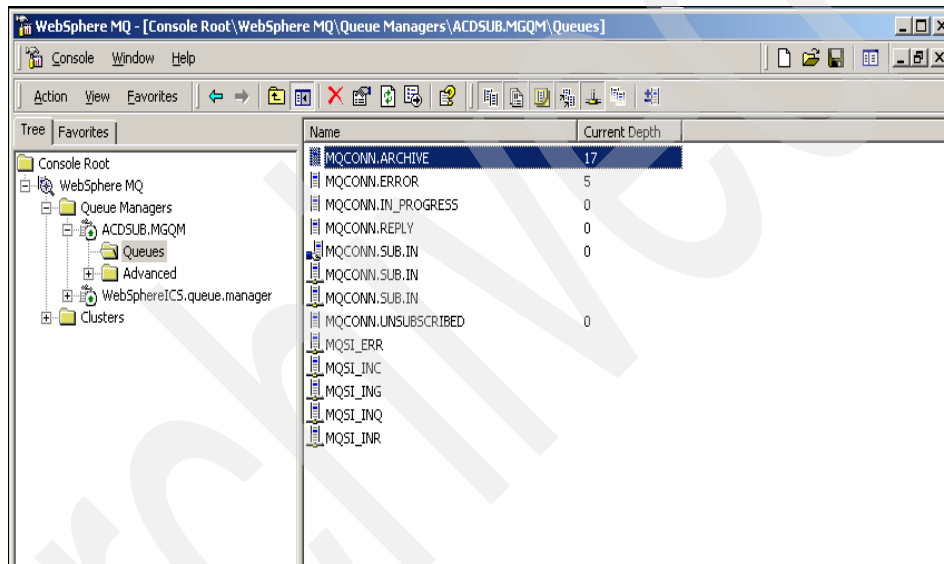


Figure 3-15 Subscriber gateway MQCONN.ARCHIVE queue

- c. Open the **Queues** folder (as shown in Figure 3-15), right-click the MQCONN.ARCHIVE queue and select **Browse Messages**.
- d. Double-click the listed message and selecting the Data tab you should be able to see data belonging to the published HL7 message, embedded in an XML envelope.

MSGID	OBSERVATIONID	SUBID	CODINGSYSTEM	DESCRIPTION
0	100-8	OBSUBID	CODESYS	DESC
1	100-8	OBSUBID	CODESYS	DESC
2	100-8	OBSUBID	CODESYS	DESC
3	100-8	OBSUBID	CODESYS	DESC
4	100-8	OBSUBID	CODESYS	DESC
5	100-8	OBSUBID	CODESYS	DESC
6	100-8	OBSUBID	CODESYS	DESC
7	100-8	OBSUBID	CODESYS	DESC
8	100-8	OBSUBID	CODESYS	DESC
9	100-8	OBSUBID	CODESYS	DESC
10	100-8	OBSUBID	CODESYS	DESC
11	100-8	OBSUBID	CODESYS	DESC
12	17012-6	OBSUBID	LOINC	INFLUENZA A AB

Figure 3-17 Example of HCNSUB.PATIENT table content

Note: For testing purposes, we created organizations, gateways, and users with full access on all the information that is published in our HCN environment. For the implementation of security and privacy policies, refer to Chapter 6, “Privacy and security” on page 165.

3.7 Chapter summary

This chapter discussed the key steps that you should take to install and configure HCN and all its components properly. It included hints, tips and practical examples to help with problem determination, installation verification, and validation and for the resolution of some common installation errors. It also presented basic suggestions regarding the correct configuration of HCN security features. For a comprehensive installation and configuration process, we encourage you to use this chapter in conjunction with the *Installation and Configuration Guide* documentation.

HCN entities and functional components

This chapter describes the key entities and functional components in the IBM WebSphere Business Integration for Healthcare Collaborative Network. It includes information about organizations, gateways, users, privacy levels, and health topics.

The chapter includes the following sections:

- ▶ HCN entities and functional components overview
- ▶ Organizations
- ▶ Gateways
- ▶ User roles
- ▶ Privacy levels
- ▶ Notifications and e-mails
- ▶ Health topics
- ▶ Chapter summary

4.1 HCN entities and functional components overview

Key to the functioning of Healthcare Collaborative Network (HCN) are a number of entities and components, as illustrated in Figure 4-1 on page 99. The set of HCN entities and components include:

- ▶ Organizations

Organizations are the highest level of entities that exist within HCN. Hospitals, pharmacies, laboratories and research establishments are examples of organizations.

- ▶ Gateways

Associated with every organizations are one or more gateways for interfacing the organization to HCN. An organization can have multiple gateways associated with it but a given gateway can be associated with only one organization.

- ▶ User roles

HCN defines a number of user roles. Associated with each user role are privileges and tasks that the user can perform. Each organization and gateway is assigned a primary user who is the main contact as well as the person who receives any organizational notifications.

- ▶ Privacy levels

The different privacy levels in HCN are used to determine the de-identification of the data that is published. Privacy levels are established for organizations and gateways.

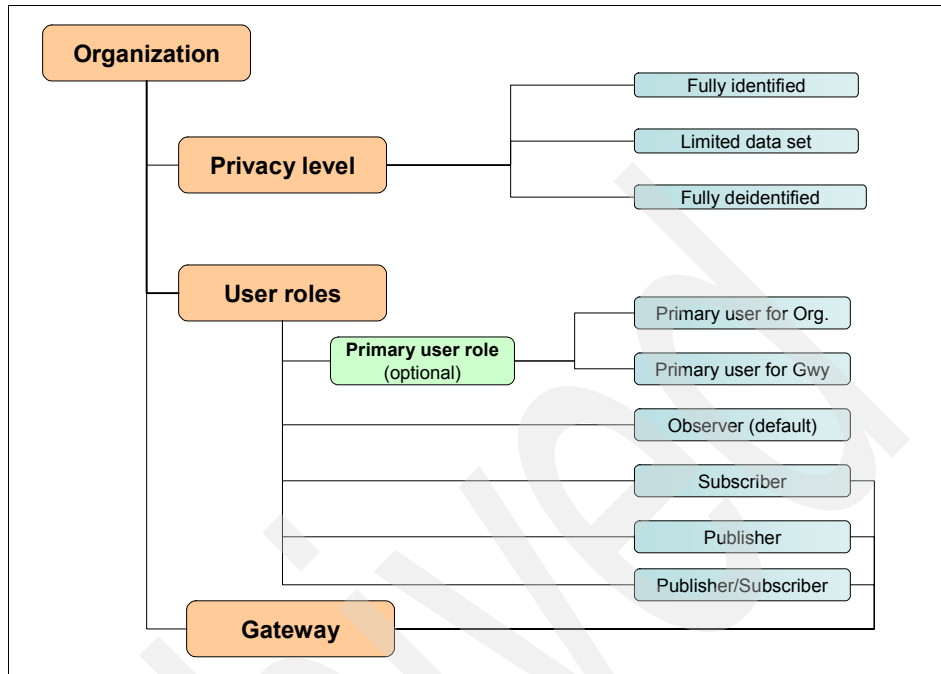


Figure 4-1 Logical representation of HCN entities and relationships

4.2 Organizations

The HCN Organization entity is used to represent hospitals, pharmacies, laboratories, research and medical centers, governmental departments and offices, as well as any other high-level institutions. An organization can have a single site or multiple physical sites. From a logical perspective, organizations are at the highest level in the hierarchy of the entities that are managed by the Administrative server application.

During the project design phase of an HCN implementation, organizations that join the network might be required to have legal agreements in place in order to share clinical information. Thus, they must agree on the privacy levels that are implemented by the network and the various organizations. Furthermore, organizations are required to indicate a single user — the primary user — to act as the point of contact for that organization. The primary user receives all organizational and non-technical notifications that the network generates.

Note: The first primary user of the organization by default is the HCN administrator (admin@hcn.com).

When creating a new organization, the HCN administrator must also specify the primary user and the associated privacy levels for which the organization is authorized to share partial or complete clinical data. For further details about how to create, update, and delete organizations, refer to 4.4, “User roles” on page 103.

After adding a new organization, the HCN administrator must associate users and gateways with the new organization for it to become operative. The HCN Administrator user can view the list of existing organizations by selecting the Organizations tab of the HCN Administrative portal application (Figure 4-2).

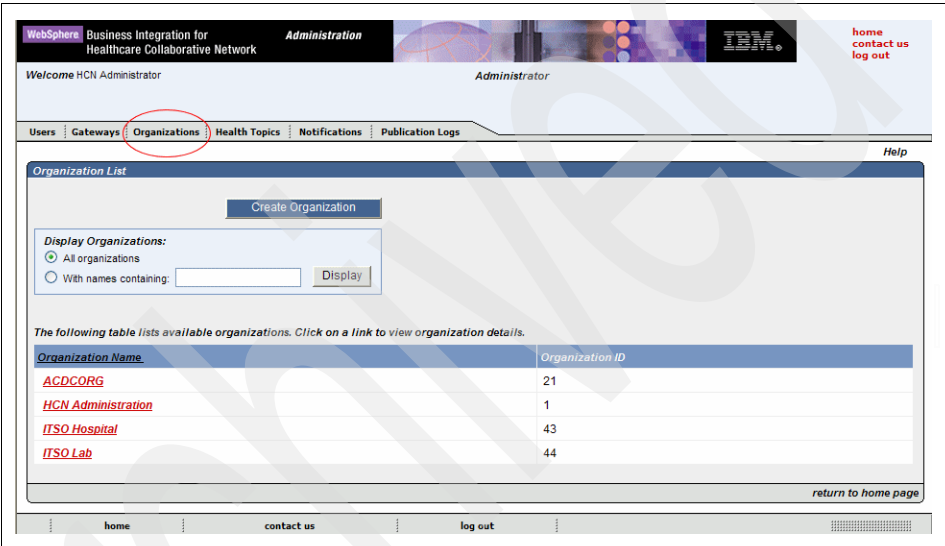


Figure 4-2 Organization list

Selecting a particular organization displays detailed information about that organization, as illustrated in Figure 4-3 on page 101.

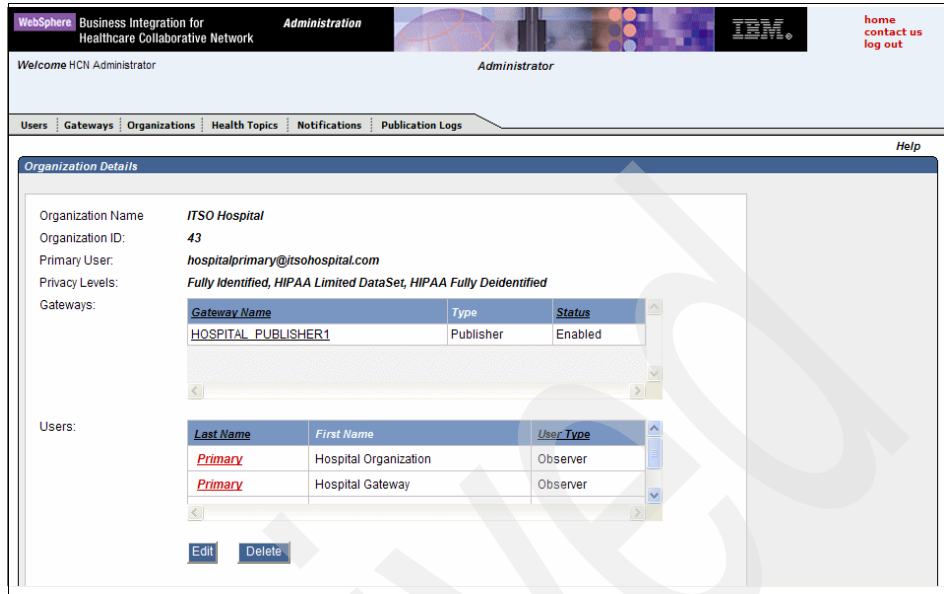


Figure 4-3 Organization details

4.3 Gateways

Gateways in HCN represent the connections between HCN and the participating organizations' IT systems. The logical gateways that are managed through the Administrative server need to be associated with the physical gateways and installed on the Gateway servers of the organization that is joining the network. From this perspective, only two kinds of logical gateways exist in HCN:

- ▶ Publisher gateways
- ▶ Subscriber gateways

A physical gateway server that acts both as publisher and subscriber must have two logical gateway entities associated with it — a publisher and a subscriber gateway.

When creating a new gateway entity, the HCN administrator must define various parameters as shown in Figure 4-4 on page 102. Notice that the gateway is associated with only one organization. Consequently, the gateway inherits the supported privacy levels from the organization.

WebSphere Business Integration for Healthcare Collaborative Network Administration

Welcome HCN Administrator Administrator

Users Gateways Organizations Health Topics Notifications Publication Logs Help

Create Gateway

* Gateway ID: HOSPPUB1

* Gateway Name: HOSPITAL_PUBLISH

* Organization: ITSO Hospital

* IP Address: 9 . 42 . 170 . 181

* Available Privacy Levels:

- ☒ Fully Identified
- ☒ HIPAA Limited DataSet
- ☒ HIPAA Fully Deidentified

* Primary User: hospitalgwprimary@itsohospital.com

* Type: Publisher

* Subscription E-mail: dryuan@itsohospital.com

Create

return to gateways page

home contact us log out

Figure 4-4 Creating gateways: Required parameters

While each gateway must be associated to one and only one organization, an organization, on the other hand, can have multiple gateways associated with it.

Note: Only subscriber gateways need a Subscription E-Mail field with the address of the person to receive e-mail notifications of clinical cases matching the published topic criteria, as shown in Example 4-1.

Example 4-1 Notification to Subscription E-Mail address of cases matching topic criteria

From: <admin@hcn.itso.ibm.com>
 To: <drlakshmi@itsoacd.gov>
 Sent: Saturday, September 10, 2005 5:28 PM

Subject: HCN Notification - Topic 'Influenza_A_H5N1_reports' has been matched

Rule triggered for topic 'Influenza_A_H5N1_reports' at
 'HOSPITAL_PUBLISHER1' on '2005-09-10T18:35:11-04:00' for patient
 'AGPI-0000000000224'.

This message has been automatically generated. Do not reply to it.
 If you have any questions or concerns, please contact the HCN administrator at
 admin@hcn.itso.ibm.com.

For information about all Administrator functions that are related to gateway management, see 4.4.1, “Administrator role” on page 104.

4.4 User roles

HCN defines a number of user roles. The roles are used to control what privileges a user has in HCN and the tasks that a given user is authorized to perform. The user roles that are defined in HCN are as follows:

- ▶ Administrator
- ▶ Subscriber
- ▶ Publisher
- ▶ Publisher and Subscriber
- ▶ Observer

While the Administrator role has the responsibility of management tasks for the whole of HCN, the Subscriber, Publisher, Observer, and Publisher and Subscriber roles are defined as *clinical roles* with specific tasks that are connected to the use of the HCN. Clinical roles should be assigned according to the functions of the individuals and of the organizations to which they belong.

In addition to the specific clinical role, a user might have a *primary user* function that has no implication on the user's operability of the network. (Note that it is possible to have primary users who have no assigned clinical roles.) Every organization and gateway in the network must have associated with it a primary user. The primary user has no specific task or functionality but acts as a focal point in HCN for the following:

- ▶ The organization — to receive administrative communications (e-mails).
- ▶ The gateway — to receive notifications (e-mails) if errors are detected in the gateway.

Note: Users can log into the HCN Administrative application at the following URL:

```
https://hostname/hcn/index.html
```

In this URL, *hostname* is the Administrative server host name. Initially, one user exists in the system (admin@hcn.com). The password for admin@hcn.com was supplied during the HCN Administrative server installation.

All user IDs in the HCN Administrative application are the user's e-mail address.

For a detailed information about user roles and tasks, see *IBM WebSphere Business Integration for Healthcare Collaborative Network - Administrators Guide*, which is available at:

<http://publib.boulder.ibm.com/infocenter/imshe1p1/v3r0/index.jsp?topic=/com.ibm.hcn.doc/hcn.html>

4.4.1 Administrator role

The administrator has the authority in HCN to manage organizations, gateways, and users. An administrator can also create topics that might be of interest to publishers and subscribers. The administrator tasks include:

- ▶ Creating, updating, and deleting organizations, users, and gateways
- ▶ Enabling and disabling gateways
- ▶ Creating and deleting topics
- ▶ Creating and deleting notifications
- ▶ Viewing publication logs for all gateways

The HCN administrator can also perform tasks from other user roles that are not administrative in nature. Table 4-1 summarizes both administrator specific tasks and those tasks that are inherited from other user roles.

Table 4-1 Administrator user tasks

Tasks	Applicable roles
Manage organizations (create, view, delete, edit)	Administrator
Manage Gateways (create, view, delete, edit, enable, disable)	Administrator
Manage users (create, view, delete, edit)	Administrator
Manage topics (create, view, delete, duplicate)	Publishers, Subscribers
View publication logs	Observers, Publishers

The default user ID for the administrator is admin@hcn.com. You cannot change or delete this ID. We suggest that you create a new user with administrator privileges and set the new user as HCN primary user to make the newly created user the HCN administrator.

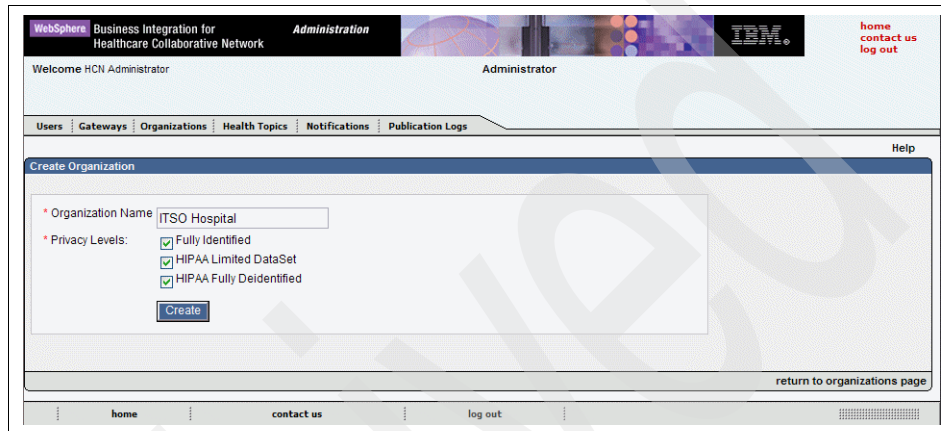
The administrator can log into the system at the following address:

`https://hostname/hcn/index.html`

In this address, *hostname* is the Administrative server host name. After the login, the HCN administrator can perform tasks as described in the sections that follow.

Managing organizations

The HCN administrator can create, view, delete, or edit organizations through the Administrative server application. Selecting **Create Organizations** within the Organizations tab of the portal home page, the administrator can create a new organization in HCN easily by adding its name and its supported privacy levels, as shown in Figure 4-5.



The screenshot shows the 'Create Organization' form within the HCN Administrator portal. The form has a header bar with 'WebSphere Business Integration for Healthcare Collaborative Network' and 'Administration' tabs. Below the header, there's a 'Welcome HCN Administrator' message and a navigation bar with 'Users', 'Gateways', 'Organizations', 'Health Topics', 'Notifications', and 'Publication Logs'. The 'Organizations' tab is selected. The form itself has a title 'Create Organization' and a 'Help' link. It contains two main sections: 'Organization Name' with a text input field containing 'ITSO Hospital', and 'Privacy Levels' with three checked checkboxes: 'Fully Identified', 'HIPAA Limited DataSet', and 'HIPAA Fully Deidentified'. A 'Create' button is located below the checkboxes. At the bottom of the form, there's a 'return to organizations page' link. The footer of the page includes 'home', 'contact us', and 'log out' links.

Figure 4-5 Administrator task: creating a new organization

If the creation is successful, the system shows a confirmation message (Figure 4-6).



The screenshot shows the 'Organization Action Confirmation' message within the HCN Administrator portal. The header bar is the same as in Figure 4-5. The navigation bar is also the same. The main content area has a title 'Organization Action Confirmation' and a red message: 'The create organization action has successfully completed.' Below the message, there's a 'return to organizations page' link. The footer of the page includes 'home', 'contact us', and 'log out' links.

Figure 4-6 Confirmation message for successful creation of new organizations

By clicking the newly created organization, the administrator can view the organization's admin default primary user (see Figure 4-7 on page 106). This page also shows any gateways and users that are associated with the organization.

WebSphere Business Integration for Healthcare Collaborative Network Administration IBM home contact us log out

Welcome HCN Administrator Administrator

Users Gateways Organizations Health Topics Notifications Publication Logs Help

Organization Details

Organization Name: ITSO Hospital
 Organization ID: 43
 Primary User: admin
 Privacy Levels: Fully Identified, HIPAA Limited Data Set, HIPAA Fully Deidentified

Gateways:

Gateway Name	Type	Status
[Search Bar]		

Users:

Last Name	First Name	User Type
[Search Bar]		

Edit Delete

Figure 4-7 Organization details: newly created organization

An administrator can also delete organizations but only if the organization has no users or gateways that are associated with it. Navigating in the organizations list (Figure 4-8), the administrator can select the organization to delete and then click **Delete** in the Organization Details page (Figure 4-9 on page 107).

WebSphere Business Integration for Healthcare Collaborative Network Administration IBM home contact us log out

Welcome HCN Administrator Administrator

Users Gateways Organizations Health Topics Notifications Publication Logs Help

Organization List

Create Organization

Display Organizations:
☒ All organizations
☐ With names containing: [Search Bar] Display

The following table lists available organizations. Click on a link to view organization details.

Organization Name	Organization ID
ACDCORG	21
HCN Administration	1
ITSO Hospital	43
ITSO Lab	44

return to home page

home contact us log out

Figure 4-8 Managing organization list

The administrator can also edit organizations by clicking the organization in the list and selecting **Edit** in the Organization Details page (Figure 4-9). The administrator can use this function to assign new users to the organization.

The screenshot shows the 'Organization Details' page for 'ITSO Hospital'. The page includes a navigation bar with tabs for Users, Gateways, Organizations, Health Topics, Notifications, and Publication Logs. The 'Organizations' tab is selected. The details for the organization are as follows:

Organization Name	ITSO Hospital									
Organization ID	43									
Primary User	hospitalprimary@itsohospital.com									
Privacy Levels	Fully Identified, HIPAA Limited DataSet, HIPAA Fully Deidentified									
Gateways	<table border="1"> <thead> <tr> <th>Gateway Name</th> <th>Type</th> <th>Status</th> </tr> </thead> <tbody> <tr> <td>HOSPITAL_PUBLISHER1</td> <td>Publisher</td> <td>Enabled</td> </tr> </tbody> </table>	Gateway Name	Type	Status	HOSPITAL_PUBLISHER1	Publisher	Enabled			
Gateway Name	Type	Status								
HOSPITAL_PUBLISHER1	Publisher	Enabled								
Users	<table border="1"> <thead> <tr> <th>Last Name</th> <th>First Name</th> <th>User Type</th> </tr> </thead> <tbody> <tr> <td>Primary</td> <td>Hospital Organization</td> <td>Observer</td> </tr> <tr> <td>Primary</td> <td>Hospital Gateway</td> <td>Observer</td> </tr> </tbody> </table>	Last Name	First Name	User Type	Primary	Hospital Organization	Observer	Primary	Hospital Gateway	Observer
Last Name	First Name	User Type								
Primary	Hospital Organization	Observer								
Primary	Hospital Gateway	Observer								

At the bottom of the page, there are 'Edit' and 'Delete' buttons.

Figure 4-9 Organization details

Managing users

The administrator can create, view, delete, and edit users from the Users tab. Creating new users requires the user's organization to exist in the system. A user is not assigned a role explicitly. Rather, the user's role is determined by the type of gateway with which the user is associated, as follows:

- ▶ A user that is associated with only one or more subscriber gateways is a subscriber user.
- ▶ A user that is associated with only one or more publisher gateways is a publisher user.
- ▶ A user that is associated with both publisher and subscriber gateways is a publisher/subscriber user.
- ▶ A user that is not associated with any gateway is an observer user.

The administrator can change a user role by associating the user with additional gateways or by removing the user from gateways.

Note: Users can only be associated to gateways from the same organization. In addition, a user can be associated with multiple gateways, and multiple users can be associated with a given gateway.

The screenshot shows the Administrator's home page with four main panels: Organizations, Gateways, Users, and Health Topics. Each panel has a 'Create' button (Create Organization, Create Gateway, Create New User, Create Topic) and a 'Display' section with radio buttons for 'All' and 'With names containing:'. The 'Create New User' button in the Users panel is circled in red. At the bottom, there are links for home, contact us, and log out.

Figure 4-10 Excerpt from Administrator's home page: Create new user

To create users, you must log into the Administrative server as the administrator and select either **Create New User** in the portal home page (as shown in Figure 4-10) or perform the same function in the Users page by selecting the Users tab (as shown in Figure 4-11 on page 108).

The screenshot shows the Users page in the WebSphere Business Integration for Healthcare Collaborative Network. The 'Create New User' button is circled in red. Below the button is a table listing available users. The table has columns for Last Name, First Name, User Type, Organization Name, Email, and Phone Number. The table lists four users: Administrator, Lakshmi, Primary, and Primary.

Last Name	First Name	User Type	Organization Name	Email	Phone Number
Administrator	HCN	Administrator	HCN Administration	admin@hcn.com	919-543-001
Lakshmi	Dr	Subscriber	ACDCORG	drlakshmi@itsoacd.gov	919-123-124
Primary	ACD Gateway	Observer	ACDCORG	acdqwprimary@itsoacd.gov	919-123-123
Primary	ACD Organization	Observer	ACDCORG	acdprimary@itsoacd.gov	919-12-123

Figure 4-11 Users page: Creating new user

The Users page shown in Figure 4-11 is how the administrator views all the defined users in the system by selecting the display criteria and clicking **Display**. The selection criteria allows the administrator to filter and sort the user list accordingly. By selecting a user from the list, the administrator views the respective user detailed information, as shown in Figure 4-12.

The screenshot shows the 'User Details' page for a user named 'Yuan, Dr' from 'ITSO Hospital'. The user's role is 'Publisher' and their email is 'dryuan@itsohospital.com'. The page includes fields for last name, first name, phone number, fax number, and a list of gateways. The gateway list has columns for Gateway Name, Type, and Status. Below the list are 'Edit' and 'Delete' buttons.

Gateway Name	Type	Status
HOSPITAL_PUBLISHER1	Publisher	Enabled

Figure 4-12 User details page.

From the User detail page the administrator can Delete or Edit the user record.

Note: A primary user must be defined for an organization or gateway at all times. To delete the existing primary user, you must first designate another user as the primary user before deleting the existing primary user.

The editing task allows the administrator to modify and update the user details, including the associated organization, associated gateways, user ID, password, name, and personal contact information (as shown in Figure 4-13 on page 110).

Users Gateways Organizations Health Topics Notifications Publication Logs Help

Update User

* Organization: ITSO Hospital

* User Role: Publisher

* User ID: dryuan@itsohospital.com

* Password: ••••••

* Confirm Password: ••••••

* Last Name: Yuan

First Name: Dr

* Phone Number: 919-123-444

Fax Number: 678657

* Gateways:

User Gateways Remove Add Gateways Add

Gateway Name	Type	Status
<input type="checkbox"/> HOSPITAL PUBLISHER!	Publisher	Enabled

Update

Figure 4-13 Update user: Editable user parameters.

Each time a user is created or the profile is updated, the user is sent a confirmation e-mail, as described in 4.6, “Notifications and e-mails” on page 136.

Managing gateways

Gateway management is similar to organization management. The HCN administrator can create, view, delete, and edit gateways. Before you create a gateway, you must have created the organization that you will associate it with.

Creating gateways

When creating a new gateway, either publisher or subscriber, you start by selecting the Gateways tab on the portal home page to go to the Gateways page. On the Gateways page, click **Create Gateway** as shown in Figure 4-14 on page 111.

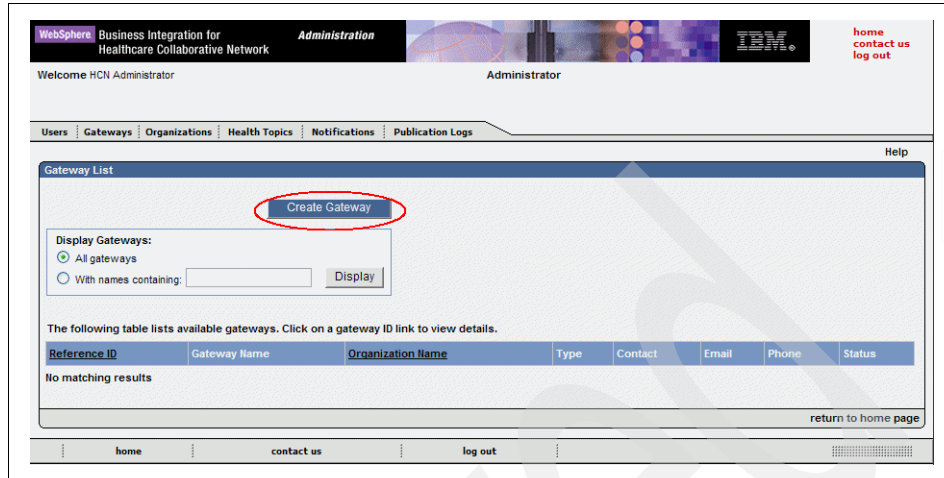


Figure 4-14 Gateway page

In the Create gateway page (Figure 4-15) include a Subscription E-mail only when you are creating a subscriber gateway. Otherwise, an error condition occurs, as shown in Figure 4-16 on page 112.

The screenshot shows the 'Create Gateway' page in the HCN Administrator interface. The form contains the following fields and values:

- Gateway ID:** HOSPUB1
- Gateway Name:** HOSPITAL_PUBLISH
- Organization:** ITSO Hospital (dropdown menu)
- IP Address:** 9, 42, 170, 181
- Available Privacy Levels:**
 - ☒ Fully Identified
 - ☒ HIPAA Limited DataSet
 - ☒ HIPAA Fully Deidentified
- Primary User:** hospitalgwprimary@itsohospital.com (dropdown menu)
- Type:** Publisher (dropdown menu)
- Subscription E-mail:** dryuan@itsohospital.c

At the bottom of the form is a 'Create' button. The footer contains 'home', 'contact us', and 'log out' links, and a 'return to gateways page' link.

Figure 4-15 Create gateway input parameters

WebSphere Business Integration for Healthcare Collaborative Network Administration IBM home contact us log out

Welcome HCN Administrator Administrator

Users Gateways Organizations Health Topics Notifications Publication Logs Help

Create Gateway

- Subscription e-mail field should be entered only for subscriber gateway type

* Gateway ID: HOSPPUB1

* Gateway Name: HOSPITAL_PUBLISH

* Organization: ITSO Hospital

* IP Address: 9 . 42 . 170 . 181

* Available Privacy Levels:

- ☒ Fully Identified
- ☒ HIPAA Limited DataSet
- ☒ HIPAA Fully Deidentified

* Primary User: hospitalgwprimary@itsohospital.com

* Type: Publisher

* Subscription E-mail: dryuan@itsohospital.com

Create

return to gateways page

Figure 4-16 Create gateway: subscriber E-mail error message

Editing gateways

After creating a gateway, we encourage you to replace the default primary user so that all the corresponding notifications are sent to a valid e-mail address. To replace the default primary user, open the Gateway Details page and edit the record by clicking **Edit** as shown in Figure 4-17 on page 113.

Users | Gateways | Organizations | Health Topics | Notifications | Publication Logs

Help

Gateway Details

Reference Code: P42
 Gateway ID: HOSPPUB1
 Gateway Name: HOSPITAL_PUBLISHER1
 Organization: ITSO Hospital
 IP Address: 9.42.170.181
 Type: Publisher
 Primary User: hospitalprimary@itsohospital.com
 Privacy Levels: Fully Identified, HIPAA Limited DataSet, HIPAA Fully Deidentified
 Subscription E-mail:
 Publications/Subscriptions:

Topics
Influenza_A_H5N1_reports
test1
Fully_Deidentified

Status: Enabled

Users:

Last Name	First Name	User Type
Werner	Dr	Publisher
Yuan	Dr	Publisher

Edit Delete Disable

Figure 4-17 Gateway details

When you are in the Update Gateways page (Figure 4-18), you can change and update the gateway information, including the IP address, primary user, subscription e-mail, and associated users.

Users | Gateways | Organizations | Health Topics | Notifications | Publication Logs

Help

Update Gateways

Reference Code: P42
 Organization: ITSO Hospital
 * IP Address: 9 42 170 181
 * Primary User: hospitalprimary@itsohospital.com
 Type: Publisher
 Selected Privacy Levels: Fully Identified, HIPAA Limited DataSet, HIPAA Fully Deidentified
 Available Privacy Levels:
 * Subscription E-mail:
 Users:

Gateway Users Remove

Last Name	First Name	User Type
<input type="checkbox"/> Werner	Dr	PUB
<input type="checkbox"/> Yuan	Dr	PUB

Add Users Add

Last Name	First Name	User Type
<input type="checkbox"/> Primarv	Hospital Organization	OBS
<input type="checkbox"/> Primarv	Hospital Gateway	OBS

Update

Figure 4-18 Edit a gateway

Enabling, disabling, and deleting gateways

Having created a gateway, the administrator needs to enable the gateway for it to exchange information within HCN. You select the gateway from the Gateway List page to get to the Gateway Details page. To enable the gateway, click **Enable** in the Gateway Details page.

Note: A fully functional publisher gateway must exist before the logical gateway on the Administrative server can be enabled. On the other hand, a subscriber gateway can be enabled even if the corresponding physical gateway, with its queue manager and queue, does not yet exist. Thus, subscriber gateways can receive e-mail subscriptions without installing a physical gateway.

The administrator can also disable gateways if the gateway is set offline for maintenance or if you are in the process of deleting the gateway. To disable a gateway, click **Disable** on the Gateway Details page.

Note: When a publisher gateway or subscriber gateway is disabled, users that are associated with this gateway no longer have the role (publisher or subscriber, respectively) that is associated with their user ID.

The administrator can delete a gateway by clicking **Delete** in the Gateway Details page only if the following prerequisites are met:

- ▶ The subscriber gateway is not subscribed to any topic.
- ▶ The publisher gateway is not currently publishing to any topic.
- ▶ The gateway is disabled.

Other tasks

As summarized in Table 4-1 on page 104, the HCN administrator can also act as a publisher, subscriber or an observer user. Thus, the HCN administrator can also perform some of the tasks of subscribers, publishers, and observers.

Note: It is not recommended that the HCN administrator assume other user roles. The administrator role is meant for management purposes rather than for clinical data exchange operations.

4.4.2 Observer role

Observer users have no operative tasks on the system. They are allowed to view only a limited set of publications, according to the organizations and gateways with which they are associated.

Viewing publication logs

Observers can only view publication logs for their associated publishing gateways. Observers can view directly the list of existing publication logs that belong to their associated organization and gateways by logging into the Administrative server portal application, which available at:

`https://hostname/hcn/index.html`

In this URL, *hostname* is the Administrative server host name. Figure 4-19 shows an example for an observer that is associated with a publishing gateway. Observers that are associated with subscribing organizations and gateways are not allowed to see any publication logs.

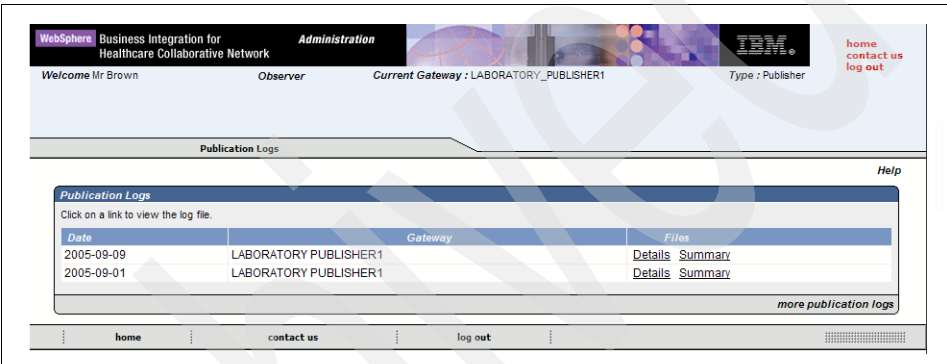


Figure 4-19 Observer home page: Publishing logs list

The log Detail link contains the HL7 messages that are sent for each publication for the day that is displayed (as shown in Example 4-2).

Example 4-2 Test published message from Publishing Hospital

Valid input message received:

Submission time: 2005-09-01 04:35:02.140

Publisher: 'HOSPITAL_PUBLISHER1'

Publish Topic: 'Constraint test 1'

Patient ID: 'LAGPI-H000000000000'

Message timestamp: '2005-09-01T16:34:23-04:00'

Message:

```
-----
'MSH|^~\&|<XXX>|<XXX>|||MSHTIME||ADT^A01|MesIDG-01.001-1|P|2.4|
EVN|A01|EVNTIME||ADM|
PID|1||LAGPI-H000000000000~IBM HCN
Gateway|||19700101|||w|~~~~~|<XXX>|<XXX>|<XXX>|||<XXX>|
PV1|1|I|<XXX>|||<XXX>|<XXX>|<XXX>|||<XXX>|||DISDISP||M||
||TIMEOFMES|TIMEOFMES|
OBX|1|ST|100-8^DESC^CODESYS|OBSUBID|7|UNITS^UTEXT^UCDSYS|REFRANGE|ABFLG|||RESST
AT||OBTIME|
```

```
DG1|1|I9|001.0^^ICD9|||A|
PR1|1||83.77^PROCDESC^I9||PRTIME|PRTYPE|1.1|||DIAGCD|
PR1|1||27620^PROCDESC^CPT4||PRTIME|PRTYPE|1.1|||DIAGCD|
,

-----
=====
Valid input message received:
Submission time: 2005-09-01 04:35:02.250
Publisher: 'HOSPITAL_PUBLISHER1'
Publish Topic: 'Constraint test 1'
Patient ID: 'LAGPI-H000000000002'
Message timestamp: '2005-09-01T16:34:23-04:00'
Message:

-----
'MSH|^~&|<XXX>|<XXX>|||MSHTIME||ADT^A03|MesIDG-01.003-1|P|2.4|
EVN|A03|EVNTIME||ADM|
PID|1||LAGPI-H000000000002^^IBM HCN
Gateway|||19700103|||w|~~~~~|<XXX>|<XXX>|<XXX>|||<XXX>|
PV1|1|I|<XXX>|||<XXX>|<XXX>|<XXX>|||<XXX>|||DISDISP||M|
||TIMEOFMES|TIMEOFMES|
DG1|1|I9|001.0^^ICD9|||A|
PR1|1||83.77^PROCDESC^I9||PRTIME|PRTYPE|1.1|||DIAGCD|
PR1|2||27620^PROCDESC^CPT4||PRTIME|PRTYPE|1.1|||DIAGCD|
OBX|1|ST|100-8^DESC^CODESYS|OBSUBID|7|UNITS^UTEXT^UCDSYS|REFRANGE|ABFLG|||RESST
AT|||OBTIME|
,
```

The summary link displays the number of publications that are sent for each published topic in the specified day.

4.4.3 Subscriber role

Subscribers in the HCN are typically oversight agencies, payers, researchers, or other interested parties whose subscription requests were authorized by publishers of the topics to receive messages. Subscribers can create and manage subscription requests. Additionally, subscribers can perform tasks within the HCN Administrative application as shown in Table 4-2.

Table 4-2 Subscriber user tasks

Task	Applicable roles
Manage topics (create, view, delete, and duplicate)	Publishers, Subscribers
Managing subscriptions (create, view, delete, and edit)	Subscriber
View gateways	Publishers, Subscribers

Similar to all the other users, subscribers can access their home page by logging into the Administrative server application, at the following address:

`https://hostname/hcn/index.html`

In this URL, *hostname* is the Administrative server host name.

Managing topics

Managing topics is a task that can be performed by publishers, subscribers, or administrators. Within these roles, you can create topics, validate user input, view topics, duplicate topics, and delete topics.

Creating topics

A subscriber can initiate the process of creating a topic from either the subscriber's portal home page, by clicking **Create Topic** (Figure 4-20 on page 117 shows a Subscriber user portal home page) or by accessing the Health Topics tab in the Health topics page.

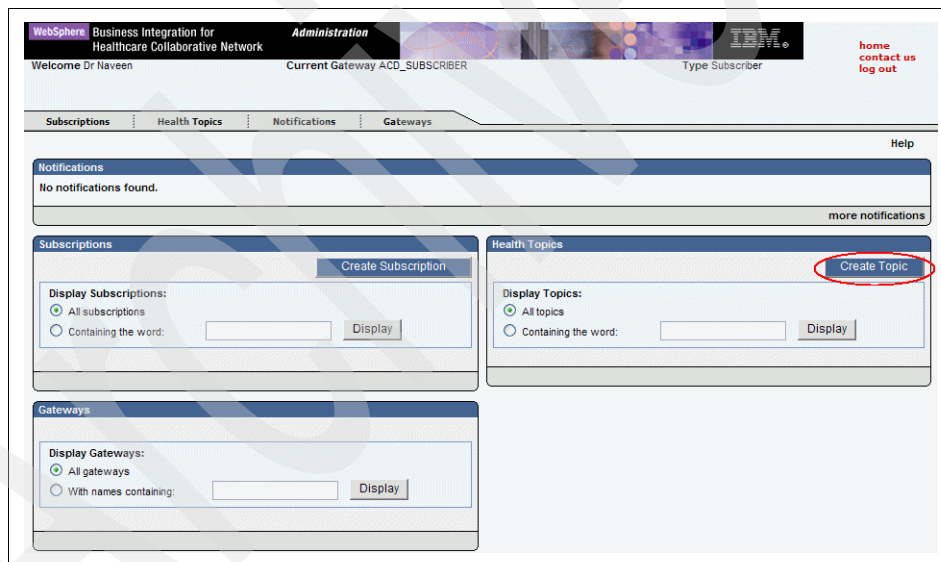


Figure 4-20 Subscriber portal home page

Within HCN you can create one of four types of topics as shown in Figure 4-21. In our scenario, we created *Public Health Alert* topics that were related to cases of *bird flu (Influenza A H5N1)*. For further details on health topics, refer to 4.7, “Health topics” on page 141.

The screenshot shows the 'Create Topic Definition' page in the HCN interface. The page has a header with 'WebSphere Business Integration for Healthcare Collaborative Network' and 'Administration' tabs. Below the header, there are navigation tabs: 'Subscriptions', 'Health Topics', 'Notifications', and 'Gateways'. The 'Health Topics' tab is selected. The main content area is titled 'Create Topic Definition' and contains a section 'Topic Definition Details'. Under this section, there is a prompt: 'Select the type of topic you would like to create.' Below this prompt are four radio button options:

- ☐ **Adverse Drug Event**
"Adverse Drug Event" topics provide data that are indicative of real or potential adverse events related to the administration of a drug
- ☒ **Public Health Alert**
"Public Health Alert" topics provide data that are indicative of real or potential outbreaks that pose a risk to the population. Examples of outbreaks of interest are communicable diseases and terrorist attacks using biological or chemical agents.
- ☐ **Quality of Care**
"Quality of Care" topics provide data that can be used to report and monitor adherence to established quality standards of care or to determine prevalence of care practices for a specified population.
- ☐ **XML Only Content (XML)**
"XML Only Content" topics can be used to forward genomic and drug trial data to a subscriber without selection rules based on triggers or constraints. The information in these topics is not correlated with clinical data about particular patients.

At the bottom left of the form, there is a 'Continue' button.

Figure 4-21 Create topic definition page: Health topic options

To create a topic, you must provide the information that is required by filling in the fields in the Create Topic Definition page as shown in Figure 4-22 on page 119. Among the various parameters, the privacy level is of particular importance. (For further details on privacy levels, refer to the 4.5, “Privacy levels” on page 135.)

Depending on the type of topic that you are creating, you might also need to define *Items of Interest*. These parameters represent the constraints that have to be met in order for a publication to be triggered for the topic. XML Only Content topics do not require definition of Items of Interest.

The screenshot shows the 'Create Topic Definition' page with the following details:

- Basic Details:**
 - Topic Name: Influenza A (H5N1) reports (Maximum 50 characters)
 - Topic Type: Public Health Alert
 - Topic Description: This topic is concerned with reports of new Influenza A (H5N1) cases within the HCN domain. All members of this HCN domain are required to submit any and all suspect H5N1 cases. (Maximum 512 characters)
 - Topic Time Limit: ☒ No limit, ☐ 14 day(s), 0 hour(s)
 - Privacy Level: **HIPAA Limited Data Set** (dropdown menu showing options: HIPAA Fully Deidentified, Fully Identified, HIPAA Limited Data Set, HIPAA Fully Deidentified)
- Items of Interest:**
 - Disease Diagnoses:
 - Lab Test Orders:

Figure 4-22 Create topic definition page: Input parameters

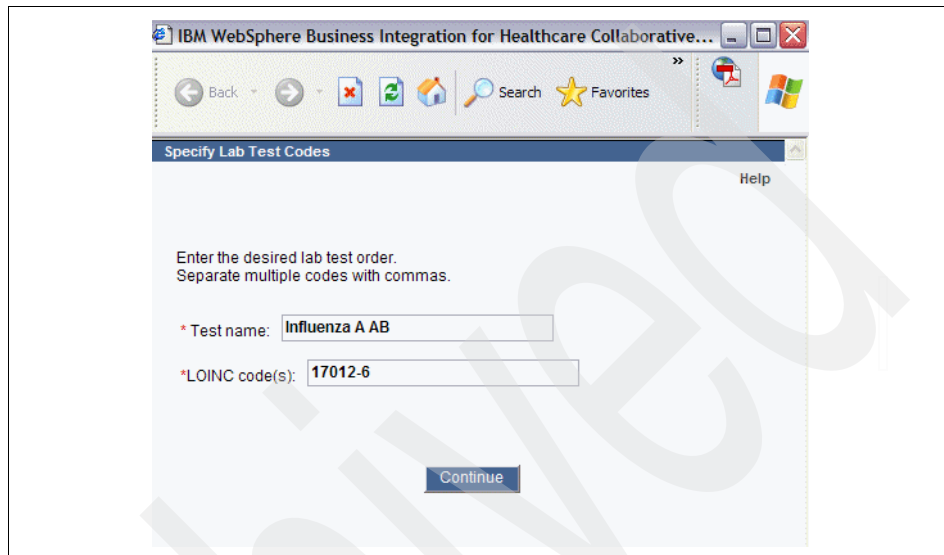
Figure 4-23 highlights the *Lab Test Order* parameter that we introduced in our scenario for the Public Health Alert on bird flu topics.

This screenshot provides a closer look at the 'Items of Interest' section of the 'Create Topic Definition' page:

- Items of Interest:**
 - Disease Diagnoses:
 - Lab Test Orders: (This button is circled in red in the original image)
 - Lab Test Results:
 - Procedure Orders:
- Patient Demographics:**
 - Gender: **Not applicable** (dropdown menu)
 - Age: ☒ Not applicable, ☐ 0 years or older, ☐ 1 years or younger

Figure 4-23 Particular of the Create Topic Definition page: Items of interest

By selecting the different constraints, a window opens to allow you to specify the values for the parameters. In the example shown in Figure 4-24, we defined the test name and the LOINC code for the laboratory order that is needed for detection of bird flu cases.



The screenshot shows a web browser window titled "IBM WebSphere Business Integration for Healthcare Collaborative...". The browser's address bar and navigation buttons (Back, Forward, Stop, Reload, Home, Search, Favorites) are visible. The main content area displays a form titled "Specify Lab Test Codes". Below the title, there is a "Help" link. The form contains the following text: "Enter the desired lab test order. Separate multiple codes with commas." Below this, there are two input fields: "* Test name:" with the value "Influenza A AB" and "* LOINC code(s):" with the value "17012-6". At the bottom of the form is a "Continue" button.

Figure 4-24 Example of laboratory test order

After you specify the parameters for the constraint, the input is validated and the item is added to the Create Topic Definition page, as illustrated in Figure 4-25 on page 121. For a description of how user inputs such as lab tests, diagnosis codes, and drug names are validated, see "Validating user input" on page 123.

Figure 4-25 Item of interest successfully added to the Create Topic Definition page

HCN allows you to add multiple items for a given constraint. For example, we could have added additional Lab Test Order items by selecting **Add Test Order** to initiate the process.

When multiple items of interest of the same type are added, you must select an operator to describe how the items must be satisfied (see the Required matches field in Figure 4-25) as follows:

- ▶ **At least 1**
This is an OR operation. Only one of the items of interest must be satisfied for the topic to be triggered.
- ▶ **At least n (where n is equal to the number of items)**
This is an AND operation. All of the items of interest must be satisfied for the topic to be published.
- ▶ **At least n (where n is less than the number of items)**
This is an at least operation. The indicated number of items must be satisfied for the topic to be published.

Items of interest for different types are always combined using an AND operation.

Important: In the Topic Description text area, do not press the ENTER key from your keyboard. Doing so produces the error that is shown in Figure 4-26.

The screenshot shows a web application interface for 'Business Integration for Healthcare Collaborative Network'. The page is titled 'Create Topic Definition'. At the top, there is a navigation bar with 'Subscriptions', 'Health Topics', 'Notifications', and 'Gateways'. A red error message at the top of the form states: 'You have entered invalid characters for the topic name or description field. You should only include characters of the following types: letter, number, dot, underscore and dash'. The form contains several fields: 'Topic Name' with the value 'Influenza_A_H5N1_reports' (Maximum 50 characters), 'Topic Type' set to 'Public Health Alert', 'Topic Description' with a long text entry (Maximum 512 characters), 'Topic Time Limit' set to 'No limit' (with options for 14 days or 0 hours), and 'Privacy Level' set to 'HIPAA Limited DataSet'. There is also a section for 'Items of Interest' with a 'Disease Diagnoses' field.

Figure 4-26 Description character error

Finally, you must specify the Payload Options that identify which messages should be included in the publication and whether the messages are published in HL7 or CDA format. The HCN Subscriber Gateway only accepts messages that are published in HL7 format. The option to publish in CDA (HL7 Clinical Document Architecture) format is included in HCN to support the IBM Clinical Genomics version 2 solution (CGv2). The CGv2 solution includes software that implements a variety of HCN Subscriber that supports receipt of XML documents, including CDA documents. For publishing messages to a standard HCN Subscriber Gateway, you should always choose the HL7 format.

When a topic is triggered on a Publisher Gateway, the gateway uses the selections on the *Include All messages of type* section of the topic creation screen to determine which messages are included in the publication. The publisher gateway applies the following rules:

1. Any message which matched an *item of interest* or implicit begin context or end context is published
2. Any message which has a time stamp between the first message that is included by rule #1 and the last message included by the first rule (ordered chronologically by time stamps) is published only if its message type was selected in *Include All message of type*.

Lab Test Results:
Add Test Result

Procedure Orders:
Add Procedure Order

Patient Demographics

Gender: Not applicable

Age: ☒ Not applicable
☐ 0 years or older
☐ 1 years or younger
☐ between 0 and 1 years (inclusive)

Payload Options

Publish HL7 Messages as: CDA For a topic published to a Clinical Genomics Repository, messages should ALWAYS be in CDA format

Include "All" messages of type: ☒ Drug Orders ☒ Lab Orders ☒ Lab Results ☒ Admission/Discharge/Transfer ☒ Procedure Orders

Create

Figure 4-27 Create Topic Definition page: payload options

After adding all the required constraints, you can create the new health topic by clicking **Create**.

Validating user input

The HCN Administration application validates the user's input for laboratory results (LOINC codes), diagnosis codes (ICD-9 CM codes), procedure codes and drug names. This validation is performed against values stored in the local database on the HCN Administrative server during installation of the Administrative server. The application does not, however, provide any selection list to allow the user to point-and-click values from a list to provide input when creating topics, due to the large number of codes in LOINC and ICD-9 CM and the large number of available drugs.

The database against which the user input is validated come from the following sources:

- ▶ LOINC: August 2002 version of LOINC from:
<http://www.regenstrief.org/loinc/>
- ▶ ICD-9 CM: 2003 version of ICD-9 CM
- ▶ Drug names: Drug database from Health Canada, 2003
- ▶ ICD-9 procedures plus CPT-4 procedures

You can customize these database tables by replacing or extending the database on the HCN Administrative Server, following the instructions in “Modifying or extending the predefined codesets” on page 207.

Viewing topics

The topics list can be accessed either through the subscriber (and publisher) user portal home page by selecting the display criteria and then clicking **Display** (Figure 4-28) or through the Health Topics tab.

The screenshot shows the HCN Administrative Server user portal. At the top, there is a header with logos for WebSphere, Business Integration for Healthcare Collaborative Network, Administration, and IBM. Below the header, there is a navigation bar with tabs for Subscriptions, Health Topics, Notifications, and Gateways. The main content area is divided into three sections: Notifications, Subscriptions, and Gateways. The Notifications section shows 'No notifications found.' with a 'more notifications' link. The Subscriptions section has a 'Create Subscription' button and a 'Display Subscriptions' section with radio buttons for 'All subscriptions' (selected) and 'Containing the word:' followed by a text input field and a 'Display' button. The Health Topics section has a 'Create Topic' button and a 'Display Topics' section with radio buttons for 'All topics' (selected) and 'Containing the word:' followed by a text input field and a 'Display' button. The Gateways section has a 'Display Gateways' section with radio buttons for 'All gateways' (selected) and 'With names containing:' followed by a text input field and a 'Display' button. The 'Display' button in the Health Topics section is circled in red.

Figure 4-28 Display topics list

Duplicating topics

Subscriber and publisher users can duplicate existing topics. Duplication of a topic is accomplished by selecting the topic from the health topics list and by clicking **Duplicate** in the corresponding Topic Details page. A new Create Topic Definition page opens and it is already pre-filled with the details and parameters of the original topic. Thus, you can either keep or modify the topic information except for the Topic Name. This feature is useful when creating a topic that differs only slightly from an existing topic.

Deleting topics

Subscriber and publisher users can delete topics by selecting a topic and clicking **Delete** on the Topic Details page.

Note: Topics cannot be deleted when:

- ▶ The topic was not created by the current user.
- ▶ The topic has subscriptions or publications that are active or pending for approval.

Managing subscriptions

When one or more topics exist, a subscriber user can create, view, edit, or delete subscriptions.

Creating subscriptions

In order to create a subscription:

1. You can do one of the following:
 - Click **Create Subscription** in the subscriber portal home page.
 - As shown in Figure 4-29, click **Create Subscription** located in the Subscriptions page, accessible through the Subscriptions tab.

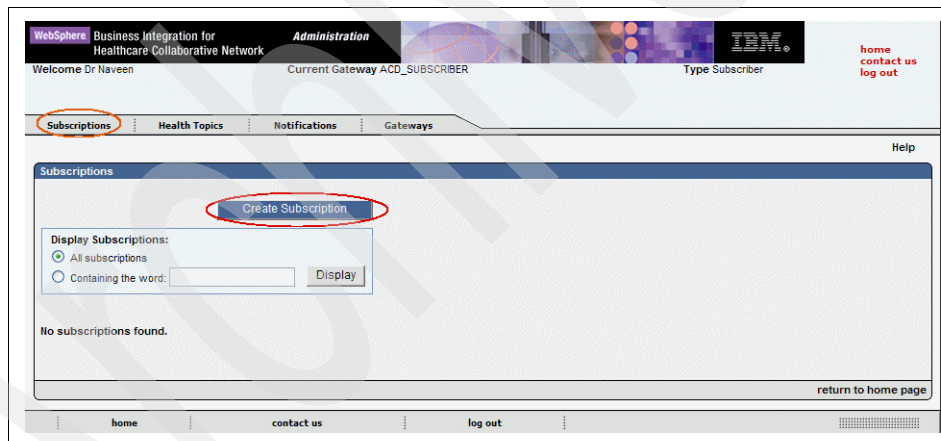


Figure 4-29 Create subscription

2. Select a topic from the topic list.
3. Select the Delivery Method in the Create New Subscription page and click **Start Subscription** (Figure 4-30 on page 126). The delivery method enables you to specify how you want to be notified when a publication on the selected topic matches the topic's constraints.

WebSphere Business Integration for Healthcare Collaborative Network Administration

Welcome Dr Naveen Current Gateway ACD_SUBSCRIBER Type Subscriber home contact us log out

Subscriptions Health Topics Notifications Gateways Help

Create New Subscription

Create New Subscription

Delivery Method:

☐ E-mail

☐ Data Transmission

☒ E-mail and Data Transmission

Start Subscription

Topic Details

Name: Influenza_A_H5N1_reports

Privacy Level: HIPAA Limited Data Set

Description: This topic is concerned with reports of new Influenza A -H5N1- cases within the HCN domain. All members of this HCN domain are required to submit any and all suspect H5N1 cases. A Center for Disease control -ACD-

Number of publishers: 1

Publishers: Click on a Gateway to view details.

Gateway: HOSPITAL_PUBLISHER1

Figure 4-30 Create new subscription: Select delivery method and start subscription

The Create Subscription Results page displays a confirmation message, as shown in Figure 4-31. The page also displays the current status of the new subscription, which can be *Approved*, *Pending Approval*, or *Denied*, depending on the Publisher's actions (see "Controlling subscription authorization requests" on page 134).

WebSphere Business Integration for Healthcare Collaborative Network Administration

Welcome Dr Naveen Current Gateway ACD_SUBSCRIBER Type Subscriber home contact us log out

Subscriptions Health Topics Notifications Gateways

Create Subscription Result

Your subscription has been successfully created. There are pending requests for publisher authorization.

Subscription Details

Subscription Status: Pending Approval

Delivery Method: Email and Data Transmission

Topic Details

Figure 4-31 Create subscription results page: Pending approval status

When you subscribe to an unpublished topic, the system generates a Publication Request to all publishers in HCN. Only when the Publication Request is approved by one or more publishers does the subscription become effective and the status is set to *Approved*.

If you attempt to subscribe to an existing topic for which you have not been pre-authorized by the publishers (see “Controlling publication requests” on page 132), the system generates and forwards Authorization Request to the publishers. Only when the request is approved by at least one publisher will the subscription becomes effective.

Tip: If you are not receiving expected publications from approved subscriptions, troubleshoot by performing the following:

- ▶ Make sure that the publications are actively being sent in the network.
- ▶ Cancel and recreate all subscriptions.

Viewing subscriptions

Subscribers can access the list of their subscriptions either from their portal home page by clicking **Display** in the Subscriptions area or by navigating to the Subscriptions page after selecting the Subscriptions tab (Figure 4-32).

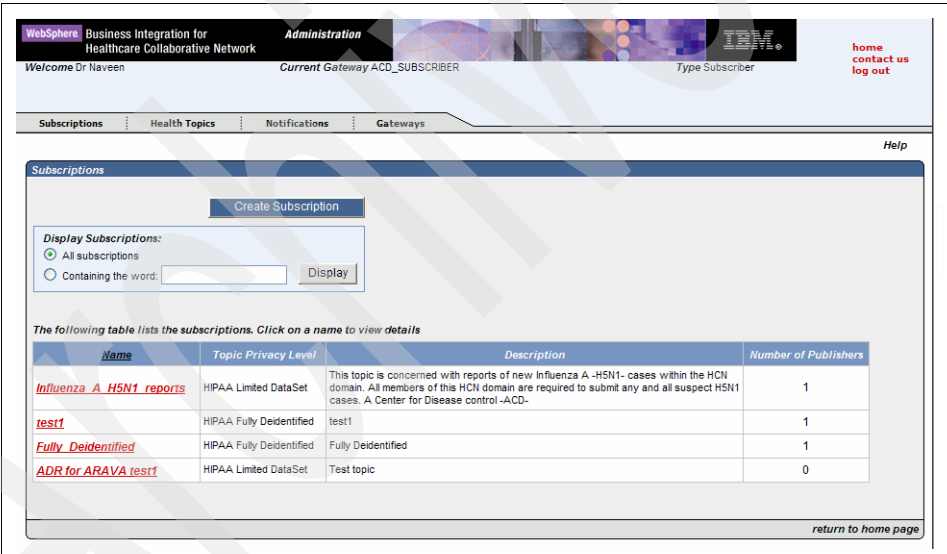


Figure 4-32 Subscriptions list

Editing subscriptions

Editing a subscription is another task that a subscriber can perform. This task can be performed after selecting the subscription by name from the subscription list (Figure 4-32). When the Subscription Details page is open, as shown in Figure 4-33 on page 128, click **Edit** to modify and update its details, essentially the Delivery Method.

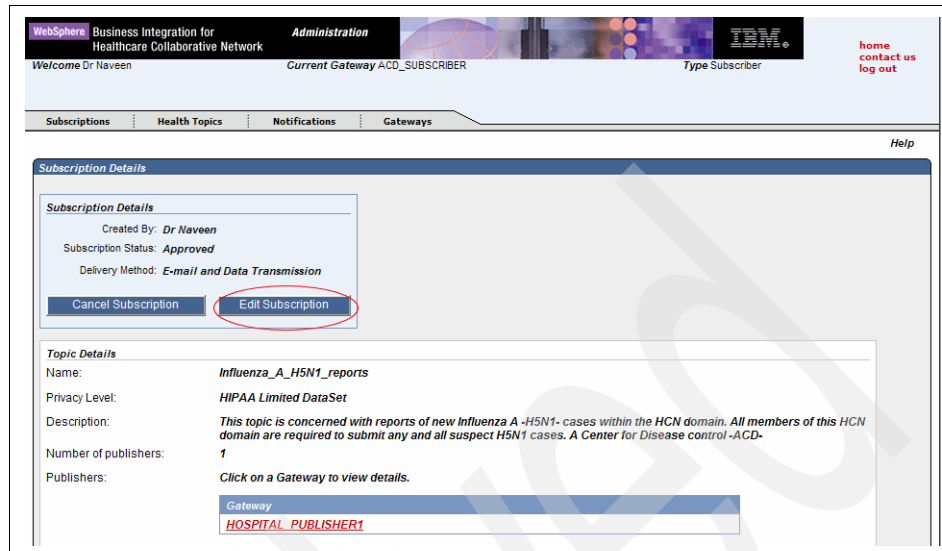


Figure 4-33 Subscription details

Deleting subscriptions

From the subscriptions list (Figure 4-32 on page 127) any subscription can be deleted by selecting its name and then selecting **Cancel Subscription** in the Subscription Details page.

Viewing gateways

You can view gateways by selecting the Gateways tab on the user portal home page or clicking **Display** in the gateways section of the same portal home page. The system displays a list showing the gateways. Note that for the current subscriber, the list shows only the publisher gateways.

4.4.4 Publisher role

Publisher users are generally associated with hospitals, laboratories, or other healthcare providers who publish clinical information in the system. A publisher can perform many tasks in the HCN portal application. Table 4-3 on page 129 summarizes these tasks.

Table 4-3 Publisher user tasks

Task	Applicable roles
Manage topics (create, view, delete, and duplicate)	Publishers, Subscribers
Manage publications (create, view, delete, edit, and control publications)	Publisher
Control publication requests	Publisher
Control subscription authorization requests	Publisher
View publication logs	Observers, Publishers
View gateways	Publishers, Subscribers

Similar to all the other users, publishers can access their portal home page by logging into the Administrative server portal application at the following address:

`https://hostname/hcn/index.html`

In this URL, *hostname* is the Administrative server host name.

Managing topics

Publishers manage topics the same way that Subscribers manage topics. For the description of the topics tasks which publisher users can perform, refer to the “Managing topics” on page 117.

Managing publications

The task of managing publications is unique to publishers. It includes creating, viewing, editing, and deleting publications.

Creating publications

You can only create publications for unpublished topics. If a topic does not exist, you must create the topic first before you can publish to it. When publishing topics for a given gateway, only those topics with a privacy level that is supported by the gateway is available for publication.

To create a publication, you can either click **Create Publication** in the **Publication** portal page or select **Create Publications** in the Publications list page (Figure 4-34 on page 130), which is accessed from the Publications tab in the same Publication portal page.

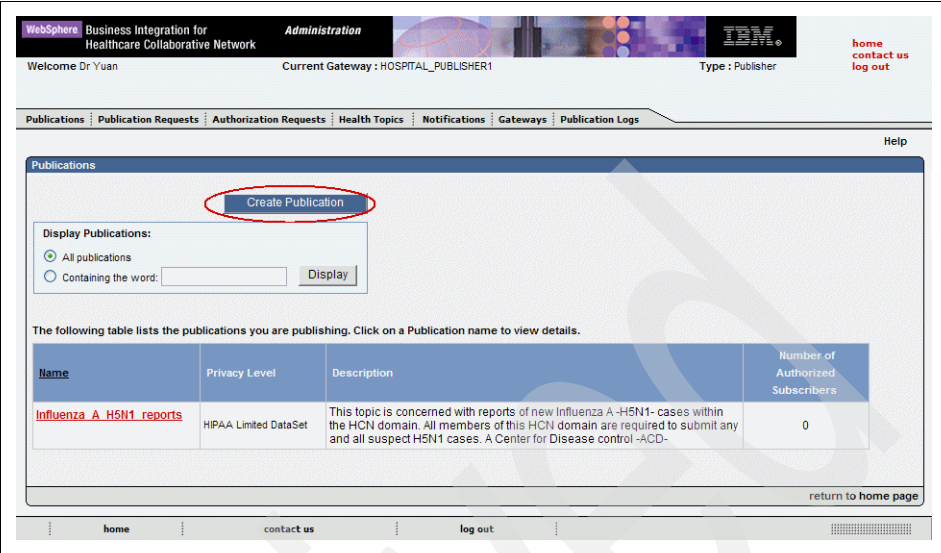


Figure 4-34 Publications list

The system displays the list of available health topics, as shown in Figure 4-35. You must select a topic from the list to create a related publication.

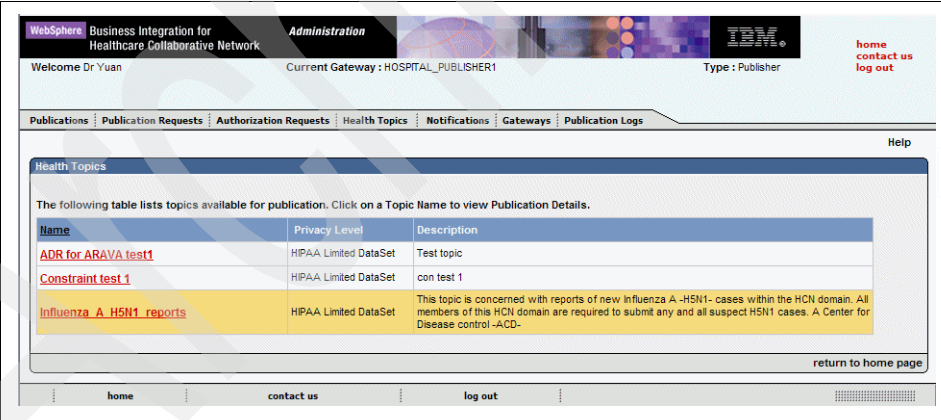


Figure 4-35 Publication creation: List of health topic

When creating a publication, you have to also decide whether to authorize subscribers to receive the publication automatically. If you choose to authorize subscribers automatically, all subscribers in the HCN system (current and future) are authorized automatically for the publication if they request it. This option is appropriate only when all participants in an HCN network are fully trusted. If this is the case, you should select **Yes** for the field Automatically Authorize Users

(Figure 4-36). Then, click **Create** in the Create New Publication page. Otherwise, you should select **No**.

If you choose not to authorize subscribers automatically, you must specify which subscriber gateways are pre-approved to receive the publication. After clicking **Create**, you select the subscriber gateways in the Select Subscribers page and then click **Approve** to create the publication. When a subscriber is pre-approved to receive a publication, data publishing commences as soon as the subscriber creates a subscription request (see “Creating subscriptions” on page 125).

The screenshot shows the 'Publication Details' page in the Healthcare Collaborative Network (HCN) interface. The page has a header with 'Welcome Dr Yuan', 'Current Gateway: HOSPITAL_PUBLISHER1', and 'Type: Publisher'. Below the header is a navigation bar with tabs: 'Publications', 'Publication Requests', 'Authorization Requests', 'Health Topics', 'Notifications', 'Gateways', and 'Publication Logs'. The main content area is titled 'Publication Details' and contains two sections: 'Publication Details' and 'Topic Details'.

Publication Details

- Created By: Dr Yuan
- Original Publication Date: 9/10/05
- Automatically Authorize Subscribers: Yes (circled in red)
- Buttons: Cancel Publication, Edit Publication

Topic Details

- Name: Influenza_A_H5N1_reports
- Privacy Level: HIPAA Limited Data Set
- Description: This topic is concerned with reports of new Influenza A -H5N1- cases within the HCN domain. All members of this HCN domain are required to submit any and all suspect H5N1 cases. A Center for Disease control -ACD-
- Number of subscribers: 1
- Subscribers: Click on a Gateway to view details.

Authorized	Gateway
Yes	ACD_SUBSCRIBER

Buttons: Display

Figure 4-36 Publication Details page

Viewing publications

Click **Display** in the Publications area of the publisher user home page or navigate to the Publications page through the Publications tab. You should see the list of Publications, as shown in Figure 4-34 on page 130. You select one of the publications for viewing by selecting the name to access the Publication Details page, as shown in Figure 4-36.

Editing publications

The only attribute of a publication that can be edited is the Automatically Authorize Subscribers field. To edit a publication, click **Display** in the Publications portal page or navigate to the Publications page using the Publications tab. Selecting the name of the publication from the list of publications that you are currently publishing displays the publication details. Click **Edit Publication** in the Publication Details page, as shown in Figure 4-36

and modify the publication details in the Update Publication Details page (see Figure 4-37).

The screenshot shows the 'Update Publication Details' page within a web application. The header includes the 'WebSphere' logo, 'Business Integration for Healthcare Collaborative Network', 'Administration' tab, 'Current Gateway: HOSPITAL_PUBLISHER1', 'Type: Publisher', and links for 'home', 'contact us', and 'log out'. A navigation bar contains 'Publications', 'Publication Requests', 'Authorization Requests', 'Health Topics', 'Notifications', 'Gateways', and 'Publication Logs'. The main content area is titled 'Update Publication Details' and contains a 'Publication Details' box with the following information: 'Original Publication Date: 9/10/05' and 'Automatically Authorize Subscribers:' with radio buttons for 'Yes' (selected) and 'No'. An 'Update' button is located below the radio buttons. A 'return to publications page' link is at the bottom right of the main content area. The footer has 'home', 'contact us', and 'log out' links.

Figure 4-37 Publication Update page

Deleting publications

You can cancel a publication by selecting a topic from the Publication list (Figure 4-34 on page 130) and then clicking **Cancel Publication** in the Publication Details page (Figure 4-36 on page 131). If a publication is canceled and then recreated, subscribers who had approved subscriptions to the publication before it was cancelled must delete their subscriptions to the topic and create a new subscription request if desired. Alternatively, the publisher can duplicate the existing topic from the cancelled publication and start publishing to the duplicated topic. The subscriber must request a subscription to the new topic in order to receive the published data.

Controlling publication requests

When a subscriber wants to subscribe to an existing topic that is yet unpublished, the corresponding publisher will be sent a Publication Request. The publisher has the authority to approve or deny the subscriber access to the data. If approved, the subscriber will immediately start receiving data published to the topic.

To approve or deny publication requests, the publisher can either select one of the requests available in the Publication Request list located in the corresponding area of his portal home page or navigate through the Publication Requests tab.

The screenshot displays the 'Publication Request Details' page. At the top, there's a navigation bar with links like 'WebSphere', 'Business Integration for Healthcare Collaborative Network', 'Administration', and 'BHIC'. Below this, a status bar shows 'Welcome Dr Yuan', 'Current Gateway : HOSPITAL_PUBLISHER1', and 'Type : Publisher'. A main navigation menu includes 'Publications', 'Publication Requests', 'Authorization Requests', 'Health Topics', 'Notifications', 'Gateways', and 'Publication Logs'. The 'Publication Request Details' section contains a form with the following fields: 'Organization Requesting Publication: ACDCORG', 'Currently Publishing to Topic: No', a 'Do Not Publish' button, 'Automatically Authorize Subscribers' with radio buttons for 'Yes' (selected) and 'No', and a 'Create Publication' button. Below this is the 'Topic Details' section, which lists: 'Name: ADR for ARAVA test1', 'Privacy Level: HIPAA Limited DataSet', 'Description: Test topic', and 'Number of subscribers: 0'. A 'Display' button is at the bottom of the topic details.

Figure 4-38 Publication request details page

In the Publication Request Details page (Figure 4-38), the publisher can choose one of the following:

- Click **Do Not Publish** to deny the Publication Request.
- Choose to authorize subscribers to receive the publication automatically. If the publisher chooses **No**, then the publisher has to select the gateways that are pre-approved to receive the publication manually by clicking **Approve** (Figure 4-39 on page 134).

If a subscriber is pre-approved for a topic, publication starts only after the subscriber requests and starts a subscription. The subscriber receives a notification of the action that was performed by the publisher.

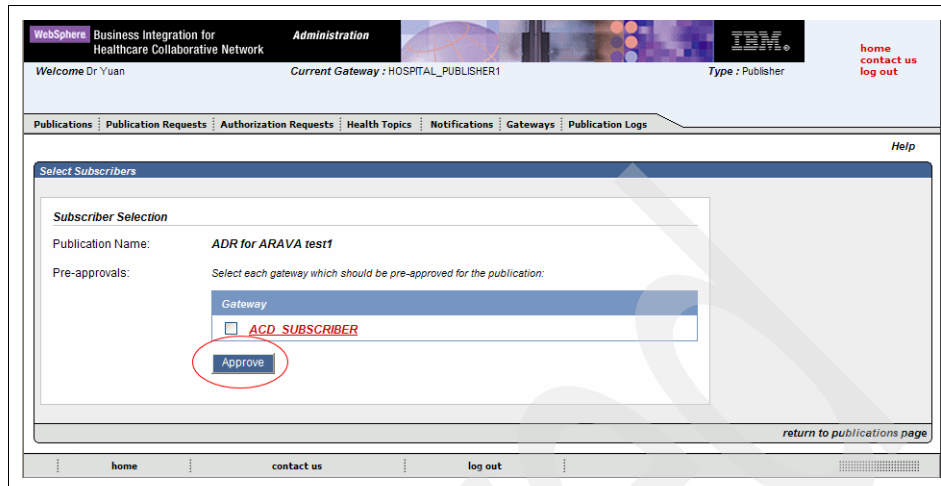


Figure 4-39 Select pre-approved subscribers

Controlling subscription authorization requests

The publisher has the authority to grant or deny subscribers access to data. When a subscriber subscribes to a topic for which he or she is not authorized, the publisher will be sent an Authorization Request. All pending Authorization Requests can be viewed in the Authorization Requests area in the portal or in the Authorization Requests page accessible through the Authorization Requests tab. On the Authorization Request screen, use Authorization Request to approve or deny an Authorization Request. The system will send the subscriber a notification of the publisher's action.

Viewing publication logs

As a publisher user, one of the tasks you can perform is that of viewing publication logs. This is similar to the viewing capabilities of an Observers. For details of how you can view publication logs, refer to “Observer role” on page 114.

Viewing gateways

Both publisher and subscriber users can view the list of gateways. However, the list that is displayed for the current publisher user only shows the subscriber gateways. To view the list of gateways, select the Gateways tab on the user portal home page or click **Display** in the gateways section of the user portal home page.

4.4.5 Publisher and Subscriber role

A participant can be both a publisher and a subscriber and as such, can both publish and subscribe to health topics. A publisher and subscriber user can perform the following tasks:

- ▶ Switch between associated publisher and subscriber gateways.
- ▶ Create and delete topics for either gateway types.
- ▶ Create, update, and delete publications for a publisher gateway.
- ▶ Authorize subscriptions to a topic for publisher gateway.
- ▶ Create, update, and delete subscription requests for a subscriber gateway.
- ▶ Subscribe to a topic for a subscriber gateway.
- ▶ View the publication logs from the publisher gateway.

As a publisher and subscriber user, you can choose which gateway you are addressing (that is, whether acting in the Publisher or Subscriber role). You then select the desired gateway from the Available Gateways and click **Change Gateways**.

For each of the tasks above, you can refer to the tasks that are associated with the single user roles (publisher or subscriber) in 4.4.4, “Publisher role” on page 128 and 4.4.3, “Subscriber role” on page 116.

4.5 Privacy levels

Privacy levels are used to describe the legal, regulatory, or contractual relationships between publisher and subscriber and the data their respective gateways can exchange. Privacy levels have the following characteristics:

- ▶ Privacy levels define what level of de-identification to be performed by the publisher gateway on messages sent to subscribers.

De-identification is the process by which any uniquely identifiable data about a patient or subject is altered or removed from the published data. Healthcare information is considered de-identified, or not individually identifiable, if it does not contain information that can identify an individual and if the organization has no reasonable basis to believe that the information can be used to identify an individual.

- ▶ Privacy levels are assigned to gateways and organizations. A privacy level assigned to an organization is an indication that the organization has a legal, regulatory, or contractual need to handle data at that level of de-identification. A privacy level of a gateway indicates that the gateway is capable of sending or receiving data at that level of de-identification.

- ▶ Topics are defined with a privacy level that defines what level of de-identification is required for a subscriber to receive a publication for that topic.
- ▶ Publishers and subscribers are only shown (and only able to create) topics that meet the privacy level they are assigned.
- ▶ The privacy level an organization is assigned is determined during the registration process of an organization.
- ▶ The set of available privacy levels are established at the organization level. A gateway can only support a privacy level if that level is supported by its associated organization.

Each privacy level is independent of any other. Although privacy levels might seem hierarchical in nature (with one privacy level providing more restrictive data access than the previous), privacy levels in no way inherit characteristics from other privacy levels. Although the default privacy levels in HCN refer to specific provisions of United States laws that are related to healthcare information security, privacy levels are completely customizable and can be tailored to any national, regional, or private security regulations. For information about how to customize privacy levels, see Appendix A, “Customizing Healthcare Collaborative Network” on page 181. For further details on privacy within HCN, refer to Chapter 6, “Privacy and security” on page 165.

4.6 Notifications and e-mails

Notifications are used to communicate significant events which have occurred within the Administrative Server application effectively and quickly. Notifications are not configurable and are generated dynamically by the HCN notification system, except for Administrative messages, which an administrative user can create. Two types of notifications are supported in HCN:

- ▶ E-Mail notifications

Typical e-mail notifications are messages sent to confirm the creation, deletion or update of a new HCN entity: user, gateway, organization. In the case of gateways an e-mail is also sent to the gateway primary user when it is enabled or disabled.
- ▶ Administrative Server internal notifications, which consists of the following types of notifications:
 - Publication/Subscription Requests
 - Authorization Requests
 - Errors
 - System Messages
 - Administrative Messages

Users can view their own notifications, delete notifications as well as view detailed messages through their portal home page or by navigating through the following tabs:

- ▶ The **Notifications** tab available to subscribers and publishers in the portal
- ▶ The **Authorization requests** tab
- ▶ The **Publication requests** tab

Figure 4-40 shows the **Create Notification** function on the HCN administrator's portal home page. It is used for the creation of an Administrative message to be sent to users.

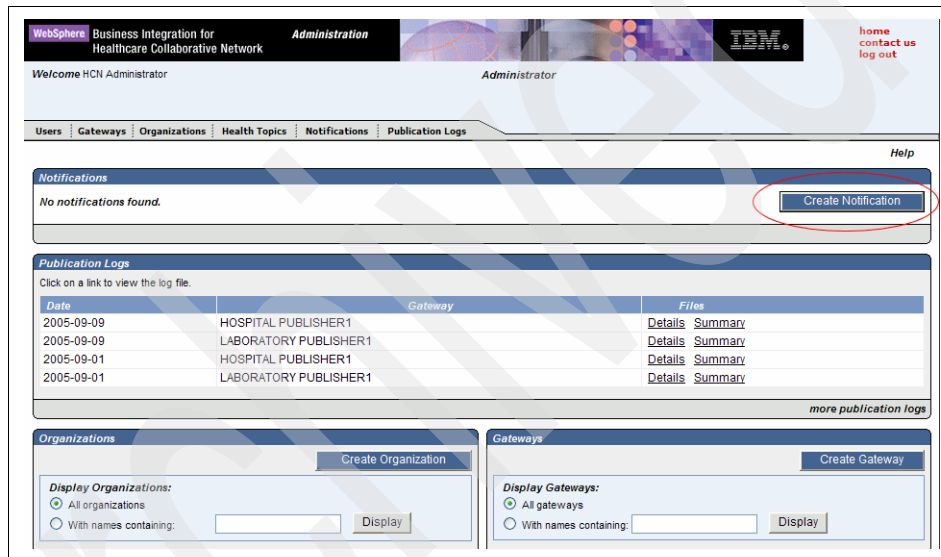


Figure 4-40 Administrator home page: Create notification

The administrator can edit the content of the notification and choose the user roles who should receive the notification: all users, subscribers, or publishers (Figure 4-41 on page 138).

The screenshot shows the 'Create New Notification' form in the HCN Administrator interface. The form has three main sections: 'To', 'Subject', and 'Message'. The 'To' section has a dropdown menu with 'All Users' selected. The 'Subject' section has a text input field with 'Publisher' entered. The 'Message' section has a large text area with 'Subscriber' entered. Below the text area are 'Create' and 'Reset' buttons. The form is titled 'Create New Notification' and has a 'Help' link. The interface includes a top navigation bar with 'WebSphere Business Integration for Healthcare Collaborative Network', 'Administration', and 'IBM' logos. A welcome message 'Welcome HCN Administrator' and 'Administrator' are displayed. A bottom navigation bar contains 'home', 'contact us', and 'log out' links. A 'return to home page' link is also present.

Figure 4-41 Create new notification: Content and receiving users

As the administrator, when you create a new notification, you receive a confirmation message, as illustrated in Figure 4-42.

The screenshot shows the 'Notification Created' confirmation message in the HCN Administrator interface. The message is displayed in a blue box with the text 'Notification Created' and 'Your notification has been successfully created.' in red. The interface includes a top navigation bar with 'WebSphere Business Integration for Healthcare Collaborative Network', 'Administration', and 'IBM' logos. A welcome message 'Welcome HCN Administrator' and 'Administrator' are displayed. A bottom navigation bar contains 'home', 'contact us', and 'log out' links. A 'return to home page' link is also present.

Figure 4-42 Notification confirmation message

When a user logs in with a role that falls in the intended receiver group, the user will see the new notification either in the notifications list on their portal home page or by clicking the Notification tab as shown in Figure 4-43 on page 139.

Selecting the corresponding notification the user can see its details in the notification details page and can eventually delete it (Figure 4-44 on page 139).

WebSphere Business Integration for Healthcare Collaborative Network Administration IBM

Welcome Dr Pietro Current Gateway : LABORATORY_PUBLISHER1 Type : Publisher

home contact us log out

Publications | Publication Requests | Authorization Requests | Health Topics | **Notifications** | Gateways | Publication Logs Help

Notifications
Click on a subject title to view the Notification Details.

Date	Time	Type	From	Subject
9/19/05	14:38	Email	admin@hcn.com	System maintenance on Sept. 20th
9/19/05	12:49	Email	admin@hcn.com	test notification
9/19/05	12:18	Email	admin@hcn.com	dfgdfgdfdfdf
9/19/05	11:45	Email	admin@hcn.com	wdfgw
9/13/05	11:23	Email	admin@hcn.com	Attention: ACD Topic created, compliance required

[more notifications](#)

Publication Requests
The following table lists requested publications.

Topic Name	Requesting Organization
test11	ACDCORG
ADR for ARAVA test1	ACDCORG
Fully Deidentified	ACDCORG
test1	ACDCORG
Influenza A H5N1 reports	ACDCORG

Authorization Requests
No requests pending.

[more authorization requests](#)

Figure 4-43 Notifications in a publisher user's home page

WebSphere Business Integration for Healthcare Collaborative Network Administration IBM

Welcome Dr Pietro Current Gateway : LABORATORY_PUBLISHER1 Type : Publisher

home contact us log out

Publications | Publication Requests | Authorization Requests | Health Topics | **Notifications** | Gateways | Publication Logs Help

Notification Detail

Date: 9/19/05
Time: 14:38
From: admin@hcn.com
Subject: System maintenance on Sept. 20th
Message: Dear users, at 11pm of Sept. 20th the system will be temporary disabled for maintenance activities. All your messages will NOT be lost.

[Delete](#)

[return to notifications page](#)

home contact us log out

Figure 4-44 Notification details

A typical system notification is sent to subscribers that are associated with a gateway when a publisher takes action on a request to receive publications on a

particular topic. Depending on the publisher's decision, subscribers receive one of the following notifications, as shown in Figure 4-45 on page 140:

- ▶ If the Publisher denied the request for publications, subscribers receive the following notification:
Requested subscription has been denied.
- ▶ If the Publisher had authorized publication of the topic to all subscribers previously, subscribers receive the following notification:
Requested publication is ready.
- ▶ If the publisher authorized the subscriber to receive publications on the topic, subscribers receive the following notification:
Requested subscription has been approved.

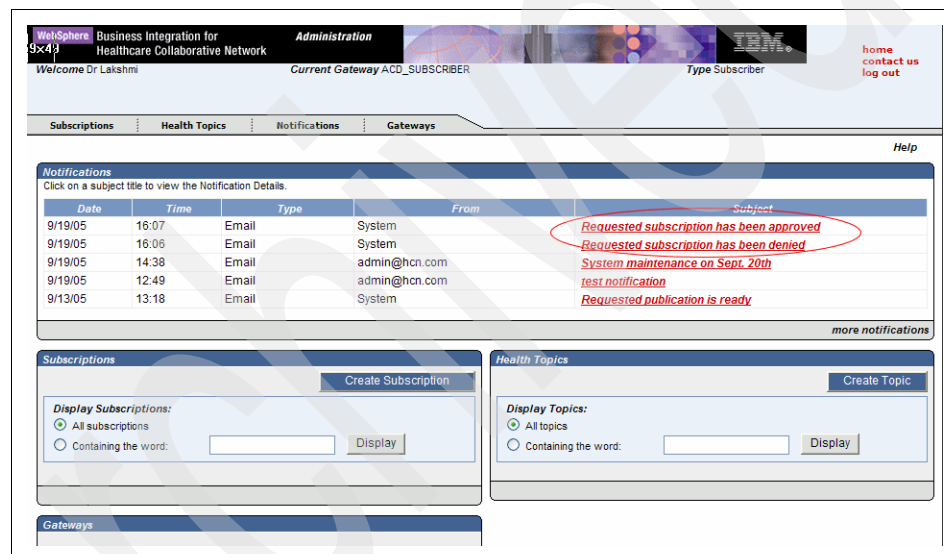


Figure 4-45 Example of subscribers' notifications on requested subscriptions

For details on publication requests, refer to "Controlling publication requests" on page 132 and "Controlling subscription authorization requests" on page 134.

When clinical information is published in HCN, the subscription e-mail address, which is defined when creating the subscriber gateway (Example 4-1 on page 102 in 4.3, "Gateways" on page 101), receives an e-mail notification that reports the clinical case that matched the published topic criteria. At the same time, the matched clinical data is sent to the subscriber's gateway message queue.

4.7 Health topics

The data flow in HCN is associated with clinical topics. Topics define areas of interest about which subscribers and publishers exchange data. In a broad sense, a topic is defined as a message or set of messages that are based on particular characteristics, such as a particular disease state, a particular laboratory or other observation, the dispensing of a particular medication, or any combination of these characteristics.

The process of creating a topic, subscribing to the topic, and publishing to the topic require the actions of several users acting in different roles. These roles are described in detail in 4.4.3, “Subscriber role” on page 116 and 4.4.4, “Publisher role” on page 128. The following steps are involved in these processes:

- ▶ A topic is defined in the Administrative server based on a selected topic protocol and includes the constraints, message filters, and other attributes which define the topic. A topic is usually created by a subscriber; however publishers can also create topics for data they possess, or an administrator can create topics on behalf of other users.
- ▶ After a topic has been defined in the Administrative server, the topic can be chosen for publication, subscription, or both.
- ▶ If a publisher chooses to publish to a particular topic, the Message flow server sends an XML message (containing the topic definition) to the Publisher gateway to inform the gateway to publish clinical messages that satisfy the constraints defined by the topic.
- ▶ If a subscriber wants to subscribe to a given topic, the subscriber must create a subscription request and send it to the publishers who are currently publishing data to the topic. If authorized by the publisher, an XML message is sent to the Message flow server to inform the Message flow server where to send any publications for this topic.

HCN includes four topic protocols, which are described in the following sections:

- ▶ Quality of Care (QOC)
- ▶ Adverse Drug Events (ADE)
- ▶ Public Health Alerts (PHA)
- ▶ XML Only Contents

4.7.1 Quality of Care

HCN can provide data that can be used for Quality of Care reporting and quality improvement activities both internal and external to a healthcare organization. HCN can support a variety of Quality of Care reporting scenarios including:

- ▶ Identification of patients for whom care deficiencies exist
- ▶ Determination of a provider's adherence to established quality of care standards or protocols
- ▶ Development of best practice guidelines for specific patient populations
- ▶ Determination of the prevalence of care practices for a specific patient population
- ▶ Identification of candidates for research, clinical trials, and disease management programs

HCN implements two approaches to Quality of Care reporting. One approach is to design topics to identify patients who meet specific quality-related criteria and provide *alerts* as soon as the condition is known, allowing the receiver to take action in a timely manner.

This approach is especially useful for hospital participants to identify specific care deficiencies for individual patients and enable action to be taken to correct a deficiency. For example, if an Acute Myocardial Infarct (AMI) patient did not receive an Angiotensin-converting Enzyme (ACE) inhibitor, the hospital could be alerted, review the chart to determine if the patient should have received the medication, and take the action dictated by the review. This approach would also be useful to identify candidates for external and internal disease management and safety programs or for medication trials. For example, a patient care department could be alerted when an elderly patient is prescribed sedatives so that they can assure that fall-prevention measures are in place. Note that in this scenario, the publisher and the subscriber could belong to the same organization, as long as that organization has both a logical publisher gateway and a logical subscriber gateway (both of which could reside on the same physical gateway).

In defining topics for the alert approach to Quality of Care monitoring, the topic is created by specifying a medication or diagnosis as clinical selection criteria, optional additional criteria (observation, procedure order, or medication order) as desired, and an evaluation time limit. HCN sends the alert to the subscriber as soon as the specified patient selection criteria are met (within the time limit) so the deficiencies can be corrected in a timely manner. The subscriber should specify a privacy level that provides sufficient identifying information to facilitate taking action on the patient's behalf.

The second approach is to design a topic to *send all available data for all patients* with a specified diagnosis or medication prescription. When this approach is used, participants can import HCN data into their own analytic systems to perform retrospective quality monitoring of multiple quality measures or perform more general research. When taking this approach, the topic is created without an evaluation time limit. The HCN Administrative server implicitly adds an end context criteria of “patient discharge” (an ADT A03 HL7 event) to the topic definition. As a result of this end context criteria, publications under these quality of care topics are published only after the patient encounter is completed. For a hospitalization, this corresponds to the discharge from the hospital.

For both approaches to quality of care topics, the HCN Administrative server implicitly creates a begin context of “patient admission” (an ADT A01 HL7 event). So for quality of care topics, only messages within a patient encounter (a hospital stay, for example) are evaluated. This prevents clinical events which occur across multiple patient encounters from being considered when a quality of care topic is evaluated.

In many clinical settings, diagnoses are not encoded using ICD-9 CM or ICD-10 codes except as part of the billing process, often after the patient encounter has completed. To account for this situation, HCN will consider an HL7 message which contains a diagnosis code received after the end of an encounter to belong to the most recent patient encounter when evaluating quality of care topics.

4.7.2 Adverse Drug Events

Adverse Drug Event topics provide data that is indicative of real or potential adverse events related to the administration of a drug. HCN supports several different HL7 message types within the pharmacy domain, including the following:

- ▶ ORM — a generic order message
- ▶ OMP — pharmacy order message (representing the order as sent by the ordering system)
- ▶ RDE — pharmacy encoded order message (representing the pharmacy’s interpretation of the order, which reflects the medication as dispensed by the formulary)
- ▶ RDS — pharmacy dispense message

An instance of any of these message types could result in the triggering of an Adverse Drug Event topic. HCN supports multiple approaches for reporting Adverse Drug Events. One approach to Adverse Drug Event reporting is to *request real time alerts* to identify patients who exhibit abnormal lab or observation values after receiving a medication. This approach is recommended

when the data receiver wants to take immediate steps to correct the situation for the patient and for notification of public health organizations. Two possible examples are:

- ▶ Patients with a prescription for felbamate with at least two of the following present:
 - Neutrophil count less than 500 cubic millimeter
 - Platelet count less than 20000
 - Reticulocyte count less than 200 cubic millimeter
- ▶ A patient with a prescription for warfarin exhibiting an International Normalized Ratio (INR)/ Prothrombin Time lab result greater than eight.

When defining topics for the alert approach to Adverse Drug Event reporting, the topic is created by specifying a medication, one or more observation values as patient-selection criteria, and an evaluation time limit. HCN sends the alert to the subscriber as soon as the specified observation value or values is sent to HCN by the publisher's results system. The subscriber should specify a privacy level that provides sufficient identifying information to facilitate taking action on the patient's behalf. Again in this scenario, the publisher and the subscriber could belong to the same organization, as long as that organization has both a logical publisher gateway and a logical subscriber gateway (both of which could reside on the same physical gateway)

Another approach to Adverse Drug Event reporting is for the subscriber to *request all data* for an entire encounter for patients who are prescribed a specified medication. In this case, the subscriber is not alerted to the event in real time but rather receives the data after the patient encounter ends. The subscriber can import the HCN data into their organization's systems for further analysis. Examples of questions that this type of analysis might answer are:

- ▶ What is the percentage of patients receiving a specific medication that experience an Adverse Drug Event?
- ▶ What are the demographic characteristics of patients who experience an Adverse Drug Event to a specific medication?
- ▶ What abnormal lab results were experienced by patients within 24 hours of being prescribed a specific medication?

For this approach to Adverse Drug Event reporting, subscribers specify a medication prescription as the clinical event criteria and choose the types of data to be sent in the payload (ADT, lab results, lab orders, drug orders, procedure orders). By not specifying an evaluation time limit, the HCN Administrative server implicitly adds an end context criteria of *patient discharge* (an ADT A03 HL7 message). HCN sends all available data of the types requested by the subscriber when the patient encounter ends.

In both approaches to Adverse Drug Event topics, the HCN Administrative server implicitly adds a begin context criteria of the medication prescription, so any clinical messages with a timestamp prior to the time of the medication order are not considered when evaluating the topic.

Although available as an option, identified data is generally not required for this type of Adverse Drug Event analysis because the intent is to study the Adverse Drug Event or medication in more detail rather than take immediate action on behalf on the patient.

4.7.3 Public Health Alerts

Public Health Alert topics provide data that are indicative of real or potential outbreaks that pose a population risk, such as communicable diseases or terrorist attacks using biological agents.

The detection and reporting of these types of public health threats is imperative. For Public Health Alert topics, generally only demographic data sufficient to determine patterns of the outbreak, such as geographical area, is required. Similar to Adverse Drug Event topics, data for Public Health Alert topics is sent as soon as the defined clinical condition is detected to allow for early detection and response to outbreaks.

The following are some examples of Public Health Alert topics you might create:

- ▶ Patients with diagnosis of bird flu or lab results positive for Influenza A H5N1 infection
- ▶ Patients with diagnosis of anthrax
- ▶ Patients with diagnosis of respiratory viral infection or lab results positive for respiratory viral infection

Public Health Alert topics are defined through diagnosis, lab orders, lab results or procedure orders. When creating a Public Health Alert topic, the HCN Administrative application does not add begin context or end context criteria, so all messages for a patient are considered when evaluating these topics.

4.7.4 XML Only Content

XML Only Content topics can be used to forward genomic and drug trial data to a subscriber without selection rules based on triggers or constraints. The information in these topics is not correlated with clinical data about particular patients. However, the same anonymous ID will be assigned to the publication allowing the recipient's system to correlate the XML data with clinical data.

The input data for an XML Only Content topic is any XML document. HCN supports these document types without additional configuration:

- ▶ Haplotype Map (HapMap)
- ▶ MicroArray Gene Expression Markup Language (MAGE-ML)
- ▶ Bioinformatic Sequence Markup Language (BSML)
- ▶ Operational Data Model for CDISC (ODM)

The support for XML-only topics is intended to be used with the IBM Clinical Genomics version 2 solution.

4.8 Chapter summary

The chapter illustrated the main HCN logical entities: organizations, gateways, users, health topics, notifications, and privacy levels. The examples in this chapter were supported by many practical examples as well as an extensive description of user tasks, functions, and roles. Furthermore, the relationships among the different entities were presented with references to information flows and user interactions within the HCN solution.

For more information, we recommend that you read *IBM WebSphere Business Integration for Healthcare Collaborative Network - Administrators Guide*, which is available at:

<http://publib.boulder.ibm.com/infocenter/imshelp/v3r0/index.jsp?topic=/com.ibm.hcn.doc/hcn.html>

System management

This chapter provides information about managing the three main components of the HCN architecture:

- ▶ HCN Administrative and AGPI server
- ▶ HCN Message Flow Server
- ▶ HCN Gateways

In general, management of each of these components is a reflection of the techniques used to manage the underlying IBM middleware on which the component is based. Where appropriate, special considerations for an HCN deployment are discussed.

In addition, these general system management topics are discussed:

- ▶ WebSphere MQ queues and queue managers
- ▶ HCN application databases
- ▶ Backup & Recovery

This chapter includes the following sections:

- ▶ HCN Administrative and AGPI servers
- ▶ Message Flow server
- ▶ Gateway
- ▶ General system management issues
- ▶ Chapter summary

5.1 HCN Administrative and AGPI servers

The Administrative server and the AGPI server are both J2EE™ applications that run under IBM WebSphere Application Server. The standard deployment calls for both the Administrative server and the AGPI server to be installed on the same WebSphere Application Server instance, although, as we have discussed, this is not strictly necessary. General techniques for managing and troubleshooting WebSphere Application Server apply to these HCN components.

An excellent resource for system administration on WebSphere Application Server V5 is *IBM WebSphere Application Server V5.1 System Management and Configuration WebSphere Handbook Series*, which is available at:

<http://www.redbooks.ibm.com/abstracts/sg246195.html?open>

5.1.1 Log files

Log files are usually the first place to look for debugging and troubleshooting information about applications that are based in WebSphere Application Server. In addition to the standard WebSphere Application Server logs, HCN produces installation logs which can be used to troubleshoot installation problems.

You can find the installation logs for the Administrative Server and the AGPI server in the HCN root installation directory, in files named `HcnAdminServerInstallLog.txt` (for the Administrative Server) and `HcnAgpiServerInstallLog.txt` (for the AGPI server).

Table 5-1 shows log files that WebSphere Application Server generates. You can find these files in the following directory:

`<WAS_install>\WebSphere\AppServer\logs\appServerName\`

In this directory, `<WAS_install>` is the WebSphere Application Server installation directory, and `appServerName` is the name of the application server instance (usually `server1`).

Table 5-1 System log files

Log File	Remarks
<code>native_stderr.log</code>	Errors related output streams stderr and stdout.
<code>startServer.log</code>	Messages related to the starting the server instance.
<code>stopServer.log</code>	Messages related to stopping the server instance.

Log File	Remarks
SystemErr.log	The standard error stream for all Java applications within the server instance. This log will contain trace details for Java errors.
SystemOut.log	The standard output stream for all Java applications within the server instance. This log contains entries for all significant actions taken by the java applications, including the HCN Administrative server and AGPI server. In addition, this log contains system messages that are written by WebSphere Application Server.

You can find additional information about application server logs in WebSphere 5.1 at:

http://publib.boulder.ibm.com/infocenter/wasinfo/v5r1//topic/com.ibm.websphere.base.doc/info/aes/ae/ctrb_mglogs.html

5.1.2 LDAP administration

It should not be necessary for you to explicitly manage the LDAP directory that is used by the HCN Administrative Server, because the LDAP entries are managed programatically by the HCN Administrative application.

IBM Tivoli Directory Server 5.2 includes a Web-based administration tool that you can use to manage the entries in an LDAP directory if unexpected errors occur that cannot be resolved using the HCN Administrative application (provided, of course, that the user has the correct password for the Base Distinguished Name).

The Web-based administration tool, however, is not compatible with WebSphere Application Server 5.1, because it uses an imbedded version of an earlier WebSphere Application Server release. So, to use the Web-based LDAP administration tool, you must install the administration tool only (not the entire IBM Tivoli Directory Server product) on a separate system from the HCN Administrative Server, and manage the LDAP directory from this separate system.

5.1.3 Administrative server hints and tips

The following are a few hints and tips which can help you deal more effectively with some exception conditions in the Administrative Server.

Browser's back button use can result in an error page

When performing Action → Confirm → Result, use the buttons provided on the page. Using the browser's back button to get back can cause an error page to be displayed. You need to restart the action from the beginning page.

Subscriber does not receive e-mail publications

When creating a user, enter the e-mail address in the format of `userid@yourcompany.com`. Incorrect entries might be accepted. The administrator should ensure that the e-mail address is accurate, if a subscriber does not receive e-mail publications.

User does not receive e-mail notifications

The Administrative server requires a SMTP server to send e-mail notifications for processed transactions. You might get an error in the `SystemErr.log` file similar to the following:

```
[1/21/05 15:53:45:516 CST] 75d09194 SystemErr
ProcessNotificationBean 1 problem:
com.ibm.hcn.admin.core.exceptions.HCN_MessagingException - problem with
building e-mail, Caused byMailException: problem sending e-mail, Caused
byjavax.mail.SendFailedException: Sending failed; nested exception is:
javax.mail.MessagingException: Could not connect to SMTP host: localhost, port:
25; nested exception is: java.net.ConnectException: Connection refused: connect
```

Check for the value for the `mail.host` property in the `portalservices.properties` file that is located at the `lib` directory of the HCN Administrative Server installation directory. Make sure that IP address of the SMTP server is entered properly.

Error occurs when a notification is triggered

If an error occurs when a notification is triggered, the message log shows an error similar to the following:

```
2c65e651 ExceptionUtil E CNTR0019E: Non-application exception occurred while
processing method "YOUR MESSAGE". Exception data:
com.ibm.ejs.container.CreateFailureException;; nested exception is:
java.lang.reflect.InvocationTargetException.InvocationTargetException
2975848b SystemErr R ProcessNotification MDB configuration problem: problem
starting database connection, Caused byjavax.naming.NameNotFoundException: Name
"comp/env/HCNDataSource" not found in context "java:".
```

Check the value for the Database.JDBC.Datasource.Name property in the WebPortal.properties file that is located at the lib directory of the HCN Administrative Server installation directory. The value should be set to jdbc/HCNDS.

5.2 Message Flow server

The HCN Message flow server, similar to the WebSphere Business Integration Message Broker product on which it is based, requires very little administration.

5.2.1 Log files

The HCN Message flow server creates two log file in the C:\HCN directory. These files should be checked when troubleshooting problems in the HCN system. A procedure should be put in place to archive these log files on a regular basis to avoid them from taking up too much space on the file system.

The logFiler capability of the Message Flow Server creates message logs for each publisher gateway, and provides the capability to transfer those message logs to the Administrative Server. The procedure for setting up this capability in the HCN Message Flow Server Installation Guide describes how to configure the logFiler to purge old log files after a specified number of days.

5.3 Gateway

The HCN gateway is based on the WebSphere Business Integration Server Express, which is the same underlying software as the WebSphere Business Integration Server. Standard techniques for managing the WebSphere Business Integration server apply to the gateway.

An excellent resource for managing the WebSphere Business Integration Server is *Implementing and Administering WebSphere Business Integration Server V4.2.2*, which is available at:

<http://www.redbooks.ibm.com/abstracts/sg247006.html?open>

5.3.1 Gateway log files

All logging on the gateway is through the WebSphere Business Integration Server log file, which by default is located in the base WebSphere Business Integration Server installation directory.

As installed, WebSphere Business Integration Server log files grow without limit. To avoid filling the install disk with log files, you should configure the log files to use circular logging by following these steps:

1. With the WebSphere Business Integration Server running, launch the System Manager and connect to the server instance.
2. Right-click the server instance, and select **Edit Configuration**.
3. For both logging and tracing, deselect **Unlimited**, and enter a maximum size and number of archive log files. For example, you might choose 250 MB as the largest log file, and 10 as the number of archives. These sizes would consume at most 2.5 GB of disk space if you used the same file for logging and tracing or 5 GB of disk space if you used separate files for logging and tracing (Figure 5-1).

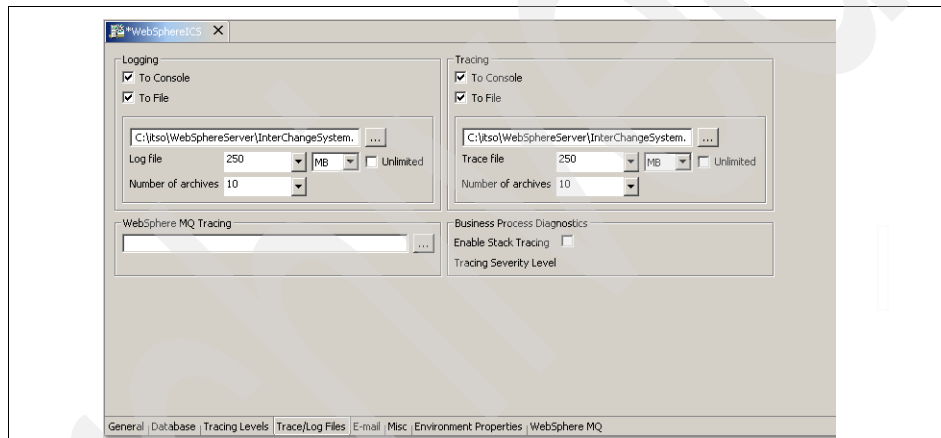


Figure 5-1 WebSphere Interchange system log file

5.3.2 Running gateway components as Windows services

In the HCN production environment, you might want to configure the HCN Gateway and connector agents to run as Windows services to avoid having to manually restart them when Windows is restarted. WebSphere Business Integration Server provides a command called **cwservice** to assist you in registering services with Windows.

Running the WebSphere Business Integration Server as a Windows service

To run the WebSphere Business Integration Server as a service, you must create two services using the **cwservice** command, one for the Persistent Name

Server used by WebSphere Business Integration Server, and one for the server itself.

The first step is to create a batch file that will be invoked when the service is launched. For the Persistent Name Server, the batch file provided by WebSphere Business Integration Server is sufficient. For the WebSphere Business Integration Server, you must take the batch file created by the HCN Gateway install and modify it work with the **cwservice** command. The batch file created by the gateway install is called `start_hcn_server.bat` and is located in the Configuration directory of the HCN installation directory.

Example 5-1 shows the contents of the modified batch. The new batch file should be named `start_hcn_server_service.bat` and should be saved in the Configuration directory. You must verify that all paths from the example (including the DOS 8.3 path names) are correct for your system.

Example 5-1 Sample start HCN server batch file

```
@echo off
setlocal

REM about to call the shared env file to set the ORB and JRE properties
call "%CROSSWORLDS%" \bin\CWSharedEnv.bat

REM Define local batch PATH to insure we execute our jre
set PATH=%JRE_BIN%;"%CROSSWORLDS%" \bin;%PATH%

REM CD to the local Crossworlds directory so we pick up
REM the java.exe and dlls required

REM Arguments: [CROSSWORLDS_ICS] [INSTALLDIR]Common\lib [PUBLISHER_GATEWAY]lib
[PUBLISHER_GATEWAY] [CHAMELEON_BASE]Java

cd /d %JRE_HOME%

set SERVERNAME=WebSphereICS

set HCN_COMMON_LIB=C:\IBM\HCN\Common\lib

set HCN_PUBLISHER_LIB=C:\IBM\HCN\PUBLIS~1\lib

set HCN_PUBLISHER_ROOT=C:\IBM\HCN\PUBLIS~1

set CHAMELEON_LIB=C:\PROGRA~1\INTERF~1\java

if "%HCN_PUBLISHER_LIB%" == "SUB" ( goto SUBSCRIBER )
:PUBLISHER
```

```

set
HCN_LIBRARIES=%HCN_PUBLISHER_ROOT%\Config;%HCN_PUBLISHER_LIB%\jakarta-oro-2.0.8.jar;%HCN_COMMON_LIB%\miracle.jar;%CHAMELEON_LIB%\classes.jar;%HCN_COMMON_LIB%\activation.jar;%HCN_COMMON_LIB%\axis.jar;%HCN_PUBLISHER_LIB%\TopicGrammar.jar;%HCN_PUBLISHER_LIB%\xml-apis.jar;%HCN_PUBLISHER_LIB%\xercesImpl.jar;%HCN_PUBLISHER_LIB%\xalan.jar;%HCN_PUBLISHER_LIB%\xmlUtil.jar;%HCN_PUBLISHER_LIB%\deidentifier.jar;%HCN_PUBLISHER_LIB%\jlog.jar;%HCN_PUBLISHER_LIB%\sfw.jar;%HCN_PUBLISHER_LIB%\CdaConstructorCodesHandler.jar

GOTO COMMON

:SUBSCRIBER
set
HCN_LIBRARIES=%HCN_COMMON_LIB%\miracle.jar;%CHAMELEON_LIB%\classes.jar;%HCN_COMMON_LIB%\activation.jar;%HCN_COMMON_LIB%\axis.jar

:COMMON
set ICSPORT=55500

REM MQ java client library path
set MQ_LIB=%MQ_LIB%

set COLLABUTILS="%CROSSWORLDS%\lib\CollabUtils.jar

set
CWCLASSES="%CROSSWORLDS%\lib\crossworlds.jar;%CROSSWORLDS%\lib\cworion.jar;%CROSSWORLDS%\lib\CodeGeneration.jar

set
DATAHANDLER="%CROSSWORLDS%\DataHandlers\CwDataHandler.jar;%CROSSWORLDS%\DataHandlers\CustDataHandler.jar;%CROSSWORLDS%\DataHandlers\RaDataHandler.jar

set XMLPARSER="%CROSSWORLDS%\lib\xerces.jar;%CROSSWORLDS%\lib\cworion.jar

set
DATADIRECT="%CROSSWORLDS%\lib\wxbase.jar;%CROSSWORLDS%\lib\wxutil.jar;%CROSSWORLDS%\lib\wxsqlserver.jar;%CROSSWORLDS%\lib\wxoracle.jar

REM DB2 jdbc driver path
set DB2_LIB=%DB2_HOME%\java

set JAVAMAIL="%CROSSWORLDS%\lib\javamail\mail.jar;%CROSSWORLDS%\lib\jaf\activation.jar

set
JCLASSES=%JAVA%;%CWCLASSES%;%DATADIRECT%;%COLLABUTILS%;%CWUTILS%;%DATAHANDLER%;%HCN_LIBRARIES%;%XMLPARSER%;%JAVAMAIL%

REM This is the -mx param value for the Interchange Server's memory heap
set CW_MEM_HEAP=512

```

REM Start the InterChange Server

```
%CWJAVA% -Djava.ext.dirs=%JRE_EXT_DIRS%;"%MQ_LIB%";"%DB2_LIB%" -Duser.home="%CROSSWORLDS%"  
-mx%CW_MEM_HEAP%m -DCW_MEMORY_MAX=%CW_MEM_HEAP% %ORB_PROPERTY% -classpath %JCLASSES%  
ServerWrapper -s%SERVERNAME% -z%ICSPORT%
```

endlocal

After creating the new batch file you must run the **cwservice** command once to create the Persistent Name Server service and once to create the WebSphere Business Integration Server service. Example 5-2 shows the example commands. Some relevant parameters to the **cwservice** command are:

- ▶ **-xi** means to create a service. Use **-xr** to remove a service.
- ▶ **-c** specifies the batch file to be executed when the service is started
- ▶ **-s** specifies the name the service is given (the **cwservice** command prepends Cw to this name)
- ▶ **-p** specifies the port number the application uses for internal communications
- ▶ **-z** specifies dependent services

Example 5-2 Sample cwservice command file

```
cwservice -xi -mode=Auto -tNAMESERVER  
-c"C:\IBM\WebSphereServer\bin\PersistentNameServer.bat" -sNameServer -p14500  
-zDB2,MQSeriesServices  
cwservice -xi -mode=Auto -tSERVER  
-c"C:\IBM\HCN\Configuration\start_hcn_server_service.bat" -sWebSphereICS  
-p55500 -zDB2,MQSeriesServices,CwNameServer
```

Running connectors as Windows services

To run connector agents as services, you must make a copy of the batch file which starts the connector agent (we suggest giving the file the same name with **_service** added before the extension), make a few modifications to remove any parameters passed to the batch file and add one parameter to the agent invocation. The steps are listed here, and a sample script for the HCNBroker connector is shown in Example 5-3 on page 156:

1. In the CONNNAME variable assignment, replace the parameter %1 with the name of the connector (excluding the ending Connector)
2. In the CONNDIR variable assignment, replace the parameter %1 with the name of the connector (excluding the ending Connector)
3. In the SERVER variable assignment, replace the parameter %2 with the name of the ICS (WebSphereServer, by default)

4. Add a line defining the variable AGENTPORT and assigning it a value of a unique port on the system (we recommend using values in the range 55500 through 55600).
5. Modify the %CWJAVA% command to include the following:

 -z%AGENTPORT%

 Precede %3 near the end of the command invocation (include spaces before and after the additional parameter).
6. Remove the pause command if one exists at the end of the batch file.

Example 5-3 Sample start_WebSphereMQ_service.bat file

```
@echo off
call %CROSSWORLDS%\bin\CWConnEnv.bat
setlocal

REM set the name to be the application connector that is starting
set CONNNAME=HCNBroker
set CONNPACKAGENAME=com.crossworlds.connectors.WebSphereMQ.ConnectorAgent

REM set the directory where the specific connector resides
set CONNDIR="%CROSSWORLDS%\connectors\HCNBroker"

REM goto the connector specific drive & directory
cd /d %CONNDIR%

REM set the server name to be the interchange that is being targeted
set SERVER=WebSphereICS

set AGENTPORT=55504

set AGENT=%CONNDIR%\CWWebSphereMQ.jar

set JCLASSES=%JCLASSES%;%AGENT%

REM config file location defaults to HOME\InterchangeSystem.cfg on the local
machine

REM start the Java connector under the Java Application End
%CWJAVA% -oss10m -ms64m -mx128m %ORB_PROPERTY%
-Djava.ext.dirs="%MQ_LIB%";%JRE_EXT_DIRS%
-Djava.library.path="%CROSSWORLDS%\bin;%CONNDIR%";"%MQ_LIB%"
-Duser.home="%CROSSWORLDS%" -cp %JCLASSES% AppEndWrapper -l%CONNPACKAGENAME%
-n%CONNNAME%Connector -s%SERVER% -z%AGENTPORT% %3 %4

endlocal
```

After creating and editing the start service batch file, you must issue the **cwservice** command to update the Windows registry and to cause the batch file to be executed when the service is started. Example 5-4 on page 157 shows the **cwservice** invocation for the HCNBroker connector. Some relevant parameters to the **cwservice** command are:

- ▶ **-xi** means to create a service. Use **-xr** to remove a service
- ▶ **-c** specifies the batch file to be executed when the service is started
- ▶ **-s** specifies the name the service will be given (the **cwservice** command prepends Cw to this name)
- ▶ **-i** specifies the name of the WebSphere Business Integration Server instance
- ▶ **-p** specifies the port number you specified in the AGENTPORT variable in the batch file
- ▶ **-z** specifies a dependent service, in this case, the service for starting the WebSphere Business Integration Server

Example 5-4 Sample cwservice invocation

```
rem cwservice -xi -mode=Auto -tCONNECTOR
-c"C:\IBM\WebSphereServer\connectors\HCNBroker\start_WebSphereMQ_service.bat"
-sHCNBroker -iWebSphereICS -p55504 -zCwWebSphereICS
```

5.3.3 Gateway tracing

Each component of the HCN Gateway can be traced individually, and this tracing should be sufficient in most cases to identify problems on the gateway. Both collaborations and connectors in HCN Gateway support trace levels from 0 (no tracing) to 5 (verbose tracing).

To set the trace on the collaboration, you must access the collaboration properties of the collaboration object through the System Manager. Each collaboration object has two tracing properties, one to control the *system* tracing level (the flow through the collaboration) and the other one to control the trace statements within the collaboration logic. Both traces can be rather verbose, and should only be set to their highest level (5) for debugging a flow consisting of a single message or, at most, a small number of messages.

Note: Due to an issue in the System Manager, you must modify the collaboration trace levels in the Integration Component Library, and then deploy the collaboration to the WebSphere Business Integration Server again. See “Preparing the HCN development environment” on page 182 for details.

A WebSphere Business Integration connector consists of two components: a connector *agent* that runs in its own JVM™ and communicates with the target application, and a connector *controller* that runs in the same virtual machine as the WebSphere Business Integration Server. Each component can be traced individually.

To set the connector controller trace level, modify the `ControllerTraceLevel` in the connector properties through the WebSphere Business Integration Server Component Manager. The `ControllerTraceLevel` change should be applied immediately.

The agent trace level is configured in the same manner by modifying the `AgentTraceLevel` property. By default, the connector agent traces to standard output, which will not be captured if the connector agent is configured to run in the background as a windows service. Even when the connector agent is running in the foreground, trace information is likely to be lost (by scrolling out off the command window) when running at higher trace levels.

The `LogFileName` and `TraceFileName` properties accessed through the Connector Configurator do not work to control the location of the log or trace files. To trace a connector agent to a file, you must use a connector agent configuration file as follows:

1. In the root directory for the connector (under `IBM\WebSphereServer\connectors`), create a configuration file with the same name as the connector and the extension `.cfg`.
2. Put the text shown in Example 5-5 in the configuration file (substituting the desired values of `xxx` and `yyy`).

Example 5-5 Sample configuration file

```
[LOGGING]
LOG_FILE=xxx
[TRACING]
TRACE_FILE=yyy
```

3. Modify the shortcut that is used to start the connector agent. At the end of the Target, add a space and then `-c` followed without a space by the fully qualified path name of the configuration file that you created.
4. Restart the connect agent.

Note: The WebSphere Business Integration Adaptor framework modifies the configuration file by converting it to an XML document.

5.4 General system management issues

You will find it necessary to manage the WebSphere MQ queues to ensure that messages in HCN continue to flow flawlessly. To ensure that you can continue to run your HCN solution, backup and recovery is essential. This section discusses these system management issues.

5.4.1 WebSphere MQ queues and Queue Managers

Generally, WebSphere MQ requires little management. As long as network connectivity between the various HCN components is maintained, the MQ configuration should work as intended. This section describes one management issue that might require periodic attention and lists some basic troubleshooting techniques for WebSphere MQ.

A more detailed reference on WebSphere MQ is *WebSphere Application Server and WebSphere MQ Family Integration*, which is available at:

<http://www.redbooks.ibm.com/abstracts/sg246878.html?0pen>

Gateway archive queues

One issue that requires the attention of a system administrator is the use of archive queue on the WebSphere Business Integration Server of the HCN Gateways. The default configuration of both the Publisher and Subscriber gateway is to copy messages inbound to the gateway (over MQ) to an archive queue, called MQCONN.ARCHIVE. Each WebSphereMQ queue has a maximum queue depth property, which by default is set to 5000 messages. When the queue depth of the MQCONN.ARCHIVE queue reaches it's maximum depth, an attempt to put an additional message on the queue will result in a fatal error in the HCNBroker connector, effectively removing the gateway from communications with the rest of HCN.

The MQCONN.ARCHIVE queue only contains messages that were successfully processed by the connector agent. Messages which contain formatting errors are placed by the connector agent on the MQCONN.ERROR queue. Messages that are well formatted, but for other reasons cause errors in the Gateway collaboration logic are still placed on the MQCONN.ARCHIVE queue, but the WebSphere Business Integration Server also maintains a copy of the message in its Failed Flow database where they can be resubmitted or otherwise acted upon by the WebSphere Business Integration Server Flow Manager tool.

For a Publisher Gateway, the MQCONN.ARCHIVE queue contains Start Publishing Topic and Stop Publishing Topic messages from the HCN Administrative Server. In other words, the messages contain the topic definitions that the gateway uses in its topic evaluations.

For a Subscriber Gateway, the MQCONN.ARCHIVE queue contains publications to subscribed-to topics from the various publishers. Depending on the volume of message traffic, this queue reaches its maximum depth more quickly than on a Publisher Gateway.

There are several potential approaches to dealing with this issue. Before deciding on an approach, you should ask whether or not it is necessary in your environment to have an archive of the messages sent to the gateway, and if so, how long the archive must be maintained. Since these messages were sent to the Gateway for processing by the collaboration logic, the messages (or at least the data contained in the messages) has been stored or processed by another application. For example, on a subscriber gateway, the messages might have been parsed and stored to the subscriber database.

Some approaches that you might consider for dealing with the Gateway Archive queues are:

1. Create a program or script which periodically checks the MQCONN.ARCHIVE queue and clears messages from the queue (optionally reading them and storing to a file). In conjunction with this strategy, you might choose to modify the Maximum Queue Depth property of the queue through the MQ Explorer.
2. Modify the HCNBroker connector definition to turn off the use of archiving in the connector, by removing the value from the ArchiveQueue property.

WebSphere MQ troubleshooting

Here are some suggested techniques for troubleshooting connectivity problems with the WebSphere MQ cluster used by HCN.

- Check the status of the Cluster Sender Channel and Cluster Receiver Channel in the MQ Explorer.
 - A status of *Running* indicates that the channels are active, and MQ connectivity is OK. The problem might not be with WebSphere MQ.
 - A status of *Inactive* does not necessarily indicate an MQ problem. The channel status can be set to *Inactive* because there is no activity on the channel.

Using MQ Explorer, attempt to place a test message on a clustered queue that resides on the target machine. This causes the channel to activate if connectivity is possible between the source and the target. If successful, be sure to delete the test message from the target queue to avoid errors in the HCN application running on the target server.

- A channel status of *Retrying* most likely indicates that connectivity between the source and target is disrupted.

- ▶ Verify TCP/IP connectivity between the nodes in question. The ping command is a useful option to verify basic connectivity. However, remember that some firewalls block ICMP packets and some servers are configured not to respond to ICMP requests. As an alternative, you can use the following command to verify connectivity over port 1414 (the port used by the HCN MQ cluster):

```
telnet hostname 1414
```

If successful, the telnet command will display a blank line (because the program listening on port 1414, WebSphere MQ, does not know how to respond to a telnet request). Just press Ctrl+C to terminate the telnet program. If unsuccessful, the telnet command produces a time-out or connect failed error.

- ▶ Verify the Connection Name of the Cluster Sender Channel and Cluster Receiver Channel at both the source and target. These connection names are resolved by WebSphere MQ into TCP/IP addresses for transmission. The format of the connection name is a host name or address, followed by a port number in parentheses, for example, `hcn-message-flow(1414)`.

Has there been a change to the DNS server or local `hosts` file that causes the connection name to no longer be resolved to an IP address?

- ▶ If the telnet command fails, check:
 - Is the target server running?
 - Is the WebSphere MQ service running on the server?
 - Have there been any changes in the firewall rules between the source and the target?
- ▶ If the telnet command is successful but the MQ channel status remains inactive or retrying, verify that the SSL certificates are configured properly. Have any of the certificates expired?
- ▶ Check the WebSphere MQ error logs in the following directories for additional debugging information:

```
<MQ Install Dir>\errors\  
<MQ Install Dir>\Qmgrs\<Queue Manager Name>\errors\
```

5.4.2 HCN application databases

The application databases that are used by each of the HCN components are managed by the HCN components and require little administration. This section lists a few items that might require the attention of a database administrator.

DB2 statistics

DB2 relies on statistics related to the number of rows in a table to select an optimal access strategy for queries against that table. This can have a dramatic effect on response time for tables that have a large number of rows, or for which the number of rows is updated frequently.

To cause DB2 to re-generate the statistics for a table, run the following command:

```
db2 runstats on table tablename and indexes all
```

The **runstats** command can be run while the database is active. In the HCN, some tables could see a performance benefit from periodically running the **runstats** command, as follows:

- ▶ On the publisher gateway database, HCNPUB:
 - CACHE
 - MessageTopicStatus
- ▶ On the subscriber gateway database, HCNSUB
 - Patient
 - ReceivedMsg
 - Drug
 - Diagnosis
 - Observation
 - Procedure

5.4.3 Backup and recovery

Best practices for backup and recovery of any software can be applied to the HCN solution. This section will not attempt to provide detailed instructions for performing backup, but will identify the databases and other data sources that must be backed up and stored to enable recovery from a disaster.

Each of the servers in the HCN Solution (Administrative server, AGPI server, Message Flow server, and each gateway) should have a software image taken after successful installation and verification, so the image can be restored to new hardware if necessary after a disaster. This image should include all files in the installation directory of the HCN software and underlying IBM middleware products.

Table 5-2 lists the additional databases and files that should be backed up periodically for recovery from a disaster.

Table 5-2 HCN system databases

Component	Data Source Name	Use	Location
Administrative Server	LDAP database	User database	DB2
Administrative Server	HCNDB	Application database	DB2
Message Flow server	BK-HCN	Application database	DB2
Publisher Gateway	HCNPUB	Application data, HL7 Message Cache	DB2
Subscriber Gateway	HCNSUB	HL7 Message Data	DB2

Note: The following link provides a comprehensive discussion of data backup and recovery that is provided by IBM DB2 Universal Database. The product documentation also has thorough information about database backup and recovery.

<http://www.elink.ibm.link.ibm.com/public/applications/publications/cgibin/pbi.cgi?CTY=US&FNC=SRX&PBL=SC09-4831-00>

5.5 Chapter summary

This chapter provided basic information about system administration and management for the components of the HCN system and provided references for more detailed references for the underlying IBM middleware. Best practices for management, database administration, and backup and recovery for all software systems are applicable to the HCN solution.

Privacy and security

The personal and sensitive nature of medical information make privacy and security the two most significant concerns when it comes to electronically collecting, processing, and transmitting medical information.

This chapter introduces privacy and security in HCN and discusses how it provides a trustworthy and secure electronic messaging system suitable for medical data. It contains the following sections:

- ▶ Introduction to privacy and security
- ▶ Privacy in HCN
- ▶ Security in HCN
- ▶ Privacy and security in the Public Health Alert scenario
- ▶ Chapter summary

6.1 Introduction to privacy and security

If you take a rather over simplified view of HCN, you describe it as a system for routing healthcare messages from one point to another. However, for this seemingly simple function work in a healthcare environment, the messages must be secure, and you must ensure that patient's privacy is not compromised. Participants in HCN have to access and process healthcare information with patient personal data such as medical history and hospital discharge records. HCN enforces privacy and security rules making sure that data is not only securely transmitted but also that each participant receives only the appropriate level protected health information they are authorized to receive.

HCN privacy and security implementation is based on the following identified classes for the protection of patient information:

- ▶ Privacy

Confidentiality is the protection of information so that unauthorized people, resources, and processes cannot access that information. In Healthcare, we include under confidentiality the ability to protect the patient's privacy by providing information in an anonymous way, so that some users have access to clinical information without knowing to whom that information refers.

- ▶ Security

- Integrity is the protection of information from unauthorized changes.
- Authentication is the protection of access to patient information by ensuring that users who access information are who they claim to be.
- Non-repudiation is the protection that sources of information cannot later deny having sent that information.

Note: Some definitions and background for this chapter are taken from *Official (ISC)² Guide to the CISSP Exam* available at:

www.auerbach-publications.com

6.2 Privacy in HCN

Confidentiality in HCN is maintained through several measures, including role-based access control and *anonymization* measures. The role-based access of the HCN Administration Server is described in 4.4, "User roles" on page 103. Users have access only to those publications or subscriptions which are relevant to their own organization. In addition, users can create or view only those topics that have privacy levels that their organization supports. Privacy levels are described in detail in the "Privacy levels" on page 168.

HCN also provides support for anonymization (or de-identification) to allow some users to access clinical information without knowing to whom that information refers. De-identification is entirely customizable as described in Appendix A, “Customizing Healthcare Collaborative Network” on page 181. You need to customize the de-identification processing if you publish messages that might contain information that can identify a patient in nonstandard locations.

Note: *HIPAA* is the abbreviation for the United States Health Insurance Privacy and Accountability Act (1993). HIPAA includes (among other things) privacy rules and security rules that provide the main regulatory framework for handling sensitive patient information. The IBM HCN solution was designed and implemented originally to meet a specific U.S. scenario. So, the concepts of HIPAA are reflected in the product. However, HCN is *not* a U.S. only solution. You can customize all of the security and privacy features of HCN to meet the security, privacy, and regulatory restrictions imposed on the handling of healthcare information anywhere in the world.

The HCN realization for anonymization fully supports confidentiality of health information based on the HIPAA Protected Health Information. HIPAA Protected Health Information are the individually identifiable health information that consists of 18 data elements that can be used to uniquely identify an individual, including the following:

- ▶ Names
- ▶ All geographic subdivisions smaller than a state, including street address, city, county, precinct, ZIP code, and their equivalent geocodes, except for the initial three digits of a ZIP code if, according to the current publicly available data from the Bureau of the Census:
 - The geographic unit formed by combining all ZIP codes with the same three initial digits contains more than 20,000 people
 - The initial three digits of a ZIP code for all such geographic units containing 20,000 or fewer people is changed to 000
- ▶ All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements might be aggregated into a single category of age 90 or older
- ▶ Telephone numbers
- ▶ Fax numbers
- ▶ E-mail addresses
- ▶ Social security numbers

- ▶ Medical record numbers
- ▶ Health plan beneficiary numbers
- ▶ Account numbers
- ▶ Certificate/license numbers
- ▶ Vehicle identifiers and serial numbers, including license plate numbers
- ▶ Medical device identifiers and serial numbers
- ▶ Web Universal Resource Locators (URLs)
- ▶ Internet protocol (IP) address numbers
- ▶ Biometric identifiers, including finger and voice prints
- ▶ Full face photographic images and any comparable images
- ▶ Any other unique identifying number, characteristic, or code

De-identification processing in publisher gateways remove Protected Health Information in the segments and fields of HL7 messages that are published. In addition to the default processing, HCN supports the ability for you to modify the de-identification routines, enabling you to de-identify your custom HL7 messages that include Protected Health Information.

Note: For information about how to customize privacy in HCN, refer to “Customizing HCN privacy rules” on page 211.

Privacy levels

Organizations that participate in HCN are expected to establish legal contracts between each other to enable the sharing of clinical data. HCN uses the concept of privacy levels to describe the relationship between publishers and subscribers and the data they can exchange. When organizations join HCN, they are required to specify the privacy levels they support (this could be due to legislative or legal constraints). The privacy levels are made available to the gateways associated with each organization, thereby defining the privacy level of messages that gateways can publish or subscribe to.

Anonymization in HCN makes use of three privacy levels. They are used to determine how much de-identification to apply to each publication. The first level does not apply any de-identification to the Protected Health Information data elements. All personal identifiable information is made available in the publication. The second level protects some of the Protected Health Information elements. Only a limited personal identifiable dataset is made public. The third level is fully de-identified, whereby all of the Protected Health Information elements are de-identified, making it impossible to identify the individual from the publication.

Level	Name	Description
1	Fully identified	No de-identification is applied. All “Protected Health Information” elements are exposed
2	Partially identified	De-identification is applied to some of the “Protected Health Information” elements
3	Fully de-identified	De-identification is applied to all “Protected Health Information” elements. Nothing is exposed

Figure 6-1 De-identification levels in HCN

The de-identification levels are designated as follows in data entry fields where you have to specify privacy levels in HCN:

- ▶ **FullyIdentified**
The patient ID in the original message is replaced with an anonymous token (an Anonymous Global Patient Identifier, or AGPI), but no other data is removed from the messages.
- ▶ **HIPAALimitedDataSet**
Personally identifying information in the original message is removed to conform to the Limited Data Set regulations of the U.S. HIPAA law.
- ▶ **HIPAAFullyDeidentified**
All 18 elements of Protected Health Information are removed according to the safe harbor provisions of the U.S. HIPAA law.

Privacy level dependency

A dependency relationship exists between the privacy levels supported by an organization and those of the gateways associated with the organization. That is, if an organization is created with certain privacy levels then the gateways associated with that organization will upon creation have privacy levels which are equivalent to that of the organization (note that the gateway privacy levels can be changed to be a subset of that of the organization but it cannot be a super-set of the organization’s privacy level).

For example, if an organization supports Partially Identified and Fully De-Identified privacy levels, then a gateway associated with this organization can be assigned any one of the privacy levels or both but it cannot be assigned Fully Identified because the organization does not support Fully Identified privacy level.

A given gateway (publisher, subscriber or publisher/subscriber) can be associated with one and only one organization. Users on the other hand, can be associated with multiple gateways. A user associated with a subscriber gateway will receive published topics only if the gateway's privacy levels matches that of the topic. A publisher gateway can only publish a topic only if its privacy levels match that of the topic.

Figure 6-2 summarizes the HCN privacy levels dependencies.

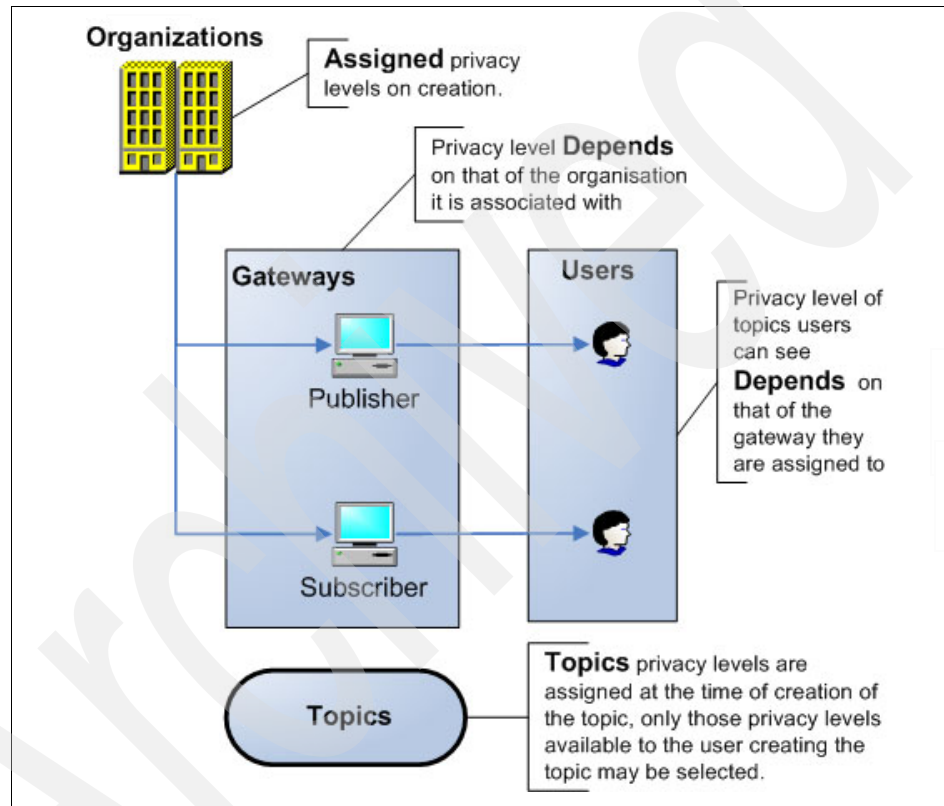


Figure 6-2 HCN privacy hierarchy

Applying privacy levels in HCN

Privacy levels are used in HCN for defining privacy policies and for de-identification processing. Three entities are at the center of privacy levels processing in HCN. These are organizations, gateways and topics. Table 6-1 on page 171 provides a summary overview showing how privacy levels are applied in HCN. Privacy levels are used primarily for de-identification processing. The publisher gateway makes use of the information entered in the definition of the

various privacy levels to apply the appropriate de-identification to messages before publication.

Table 6-1 Privacy processing in HCN

Privacy Policy	Organization	Gateway	Topic
Definition	The privacy levels that an organization supports are defined when the Organization is created in HCN.	Gateways are assigned the privacy levels of their associated organization at creation. The privacy levels can be changed at any time however, only the set of privacy levels for the associated organization are available.	The definition of a health topic includes a number of parameters one of which is the privacy levels. The privacy level is specified when the topic is created.
Processing	Not directly used in the de-identification processing. It is used to set the constraint for gateway privacy levels that must be met for publication to take place.	The publisher gateway performs the actual processing by parsing HL7 messages, performing the appropriate de-identification and creating publication messages that are sent to subscriber gateways.	The publisher gateway uses the topic privacy level de-identify the publication messages that are sent to subscriber gateways.

6.3 Security in HCN

Several messages flow through HCN. These include publications on topics from publishers to subscribers, notifications from the system administrations to users, e-mail notifications, system control and error messages (see Figure 6-3 on page 172 for a high level overview of message flow in HCN). Security implementation in HCN ensures the integrity, authentication and non-repudiation of the messages that flow in HCN. This section describes how security through integrity, authentication and non-repudiation of messages is accomplished in

HCN. For a detailed step-by-step trace of a message through HCN with description of the privacy and security processing at each step, refer to 6.4, “Privacy and security in the Public Health Alert scenario” on page 174.

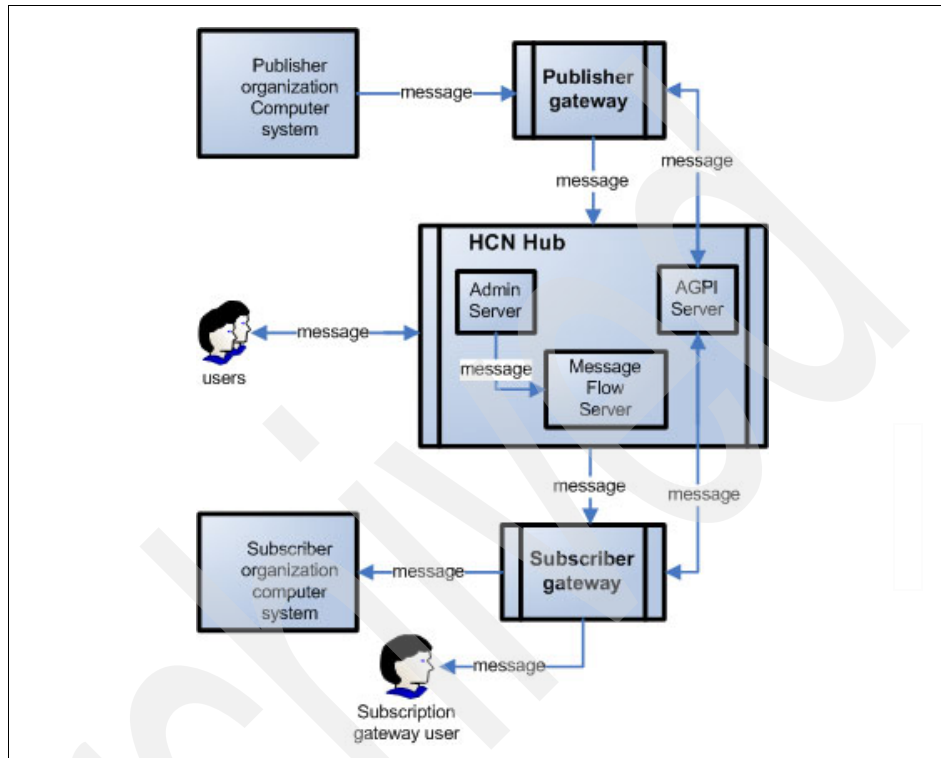


Figure 6-3 Information flow in HCN

Integrity

Integrity is maintained in HCN by the use of the Secure Sockets Layer (SSL) protocol. SSL is a public key encryption protocol, which requires two keys for encryption and decryption. The public key, which is known to everyone, is used for encrypting data, and the private key, which is known only to the recipient of the data is used for decrypting.

SSL maintains integrity through the use of a message digest. A message digest is a short code, calculated by algorithm based on the contents of the message, which is added to the end of a message prior to encryption. The receiver calculates the message digest again upon decryption, and if the message digest has not changed, then the receiver can be assured that the message itself has not been changed.

Integrity can also be compromised by unauthorized user activity; this is just one example of the inter-relatedness of these classes of security protections.

Authentication

Authentication is maintained in HCN by requiring users to log-on to the HCN Administration application to request a subscription to messages, or authorize the publication of messages. IBM WebSphere Application Server uses an LDAP registry to perform authentication to the Administration application.

The systems (in addition to users) within HCN are authenticated to each other. All messages between gateways and the HCN Hub are sent using IBM WebSphere MQ. The gateways and the HCN Hub authenticate each other using the WebSphere MQ mutual authentication feature, based on SSL. During the initial SSL handshake (when the WebSphere MQ channel is established), each side uses the public/private key pair to ensure that the other side of the channel is the intended system (that is, the private key holder). In this way, only HCN-registered Gateway systems can connect to the HCN Message Flow Server.

Non-repudiation

Non-repudiation is provided through SSL, and also through the use of logs. The use of SSL provides a built-in non-repudiation function, since the digital signature (SSL key) proves that the message was generated by the signatory. This provides one level of non-repudiation in HCN.

Each action performed by an authenticated user in the HCN Administrative server is recorded in the application log, so this log can be used to provide an audit trail of actions on Topics, Publications, and Subscriptions. The use of the Administrative server log for non-repudiation purposes implies that appropriate access control must be maintained on this file, to prevent tampering.

Additionally, the HCN Message Flow server can be configured to maintain a log of all messages sent through HCN from publishers to subscribers. The Hub can be configured to allow these log files to be accessed by users on the Administrative server. With appropriate access control of these log files (to prevent unauthorized tampering or deletion), these log files can be used for non-repudiation purposes.

6.4 Privacy and security in the Public Health Alert scenario

This section describes how the security and privacy features of HCN work in practice. We follow an HL7 message from its source inside a provider's system, through the publisher gateway and the HCN hub to the subscriber gateway. At each step, we describe the privacy and security features, as well as point out areas where additional security can be provided through means outside of HCN.

Figure 6-4 on page 175 shows the flow and data interaction for a message moving within our public health alert scenario. In the following section we will use the numbered points in the figure to elaborate on the privacy process of message transmission.

HCN implementation is based on a number of IBM middleware products. Where their security features are relevant to HCN solutions, we describe what they are and how you can use these features to implement additional security and privacy measures.

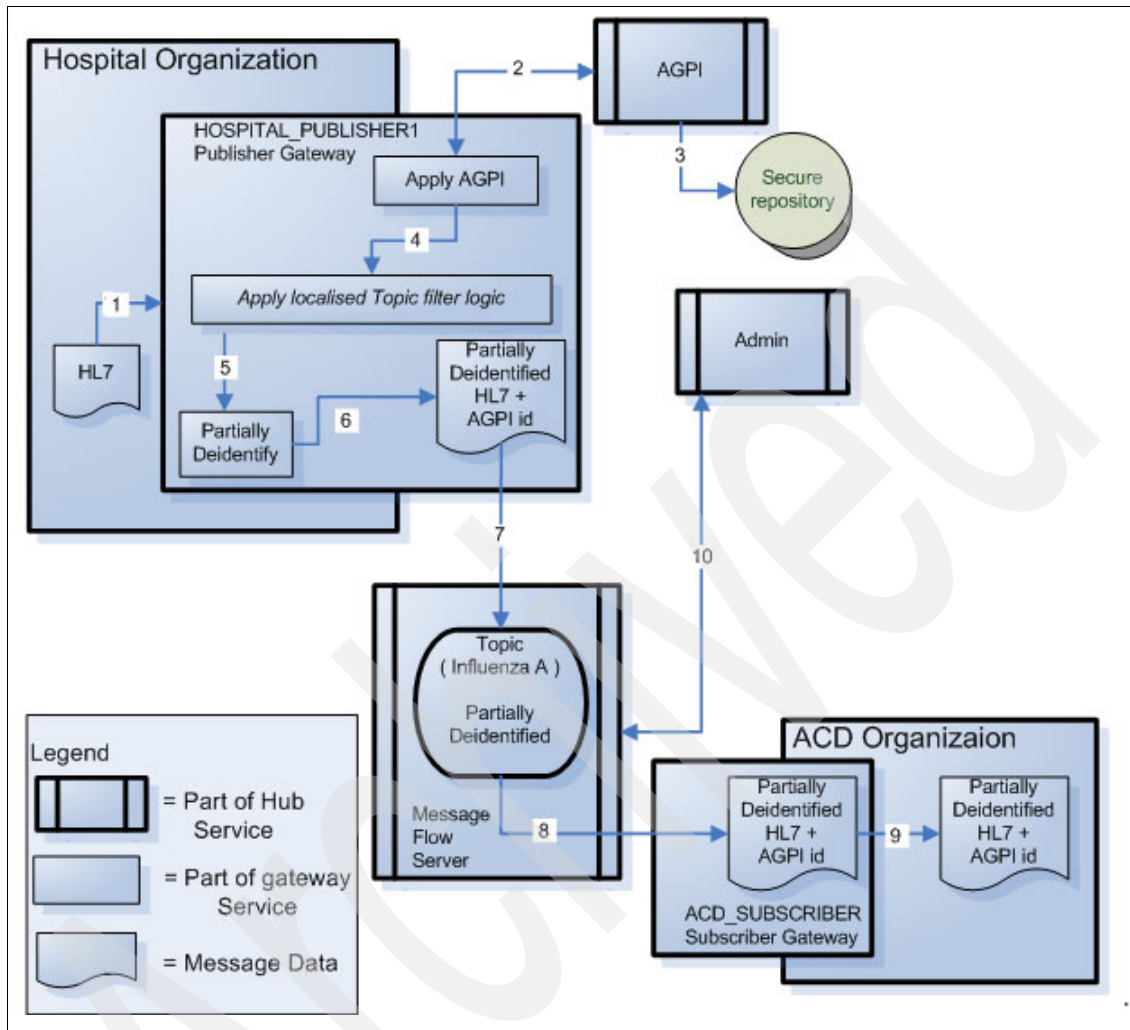


Figure 6-4 Privacy message sequences

The privacy message sequence is as follows:

1. An HL7 message is sent to the Publisher Gateway.

HCN uses WebSphere Business Integration Adapters to receive healthcare messages from healthcare provider applications. These messages are in HL7 or CDA format. HCN does not require that the messages be fully identified in order to be processed - in some cases the sending application might want to de-identify the messages prior to sending them to HCN. This possibility is catered for by loosely coupling the de-identification requirements to message processing.

The general architecture of HCN places the publisher gateway within the secure environment of the healthcare provider where the gateway server is managed under the security policies of the provider's organization. In our scenario, encrypted or protected transmission of messages from the applications to the publisher gateway was not required. Your HCN solution architecture might be such that it is necessary for you to secure the HL7 messages by sending them over a Virtual Private Network or encrypted via SSL (supported by the WebSphere Business Integration Server platform for WebSphere MQ, HTTP, or FTP transport).

In the scenario we used in this Roadbed, the link between the provider application and the publisher gateway was simulated using the file system. Our simulation application deposited HL7 messages onto the file system of the publishing gateway machine to read. The messages were in clear text with no encryption.

2. The AGPI service is invoked to assign a unique anonymous Identifier.

Upon receipt of the message, the patient-identifying information is retrieved, and the AGPI service is invoked to assign an anonymous identifier. This process is always undertaken regardless of the potential privacy requirements relating to de-identification later in the process. This is necessary to ensure that all messages for the patient will have the same identifier even if they came from different sources.

The patient-identifying information only, not the entire HL7 message, is sent to the AGPI server. Hence the information travelling between the gateway and the AGPI server has no clinical information. Nonetheless, the data travelling between these two points still needs to be protected to maintain confidentiality and integrity.

The AGPI server is invoked via Web Services, with supported bindings for SOAP over HTTP and SOAP over JMS. Each of these transports can be secured using SSL.

For our scenario, the AGPI server was invoked via SOAP over JMS. The JMS queues were implemented using WebSphere MQ with SSL.

3. Data is stored in a private and secure AGPI repository.

The AGPI service can be configured to consider different patient attributes (name, medical record number, address, phone number, address, date of birth, etc.) with different weights when matching patients for the purpose of assigning an anonymous ID. The AGPI service compares each of these attributes against the data in its database, and updates its database to save information for new patients, along with the generated anonymous ID.

The AGPI repository is a DB2 database. This database stores the patient attributes and provides the HCN infrastructure with the possibility of re-identification at some later time.

This database does not contain clinical information; however, it does contain patient attributes, including medical record numbers, phone numbers, and other information which individuals expect to remain private. As the administrator of the AGPI server, you must take appropriate security measures. At a minimum, it should include strict access control to the server and database, and auditing of access thereof. In most circumstances, remote access to this database should be disabled or restricted.

The administrator should also consider intrusion detection on the database, or encryption of the data in the AGPI server database. These techniques will provide an extra layer of confidentiality protection for data residing in the database should a breach in server security occur.

4. The messages are cached and evaluated against the topics.

When a clinical message is received, it is stored in a database cache so it can be evaluated against the set of topics being published by that gateway.

Each publisher gateway publishes one or more topics. The number of topics depends on the number of publication and subscription requests that the publisher has accepted and authorized. Each topic includes criteria that are used to determine how clinical data is filtered and packaged for publication. One of the attributes is privacy level. This specifies the level of de-identification that must be applied to publications for that topic.

The gateway makes use of all messages in the database cache for a given patient to evaluate against a topic. Some topics require multiple clinical events (in which case it requires more than one HL7 message) to be satisfied, as a result, zero or more “publication messages” can be produced. Each publication message is an XML document that contains one or more clinical (HL7) messages in its payload.

Evaluation of messages against topics does not present additional security or privacy issues. The fact that clinical messages are stored in the database cache implies that strict access control must be in place for the server. In most circumstances, remote access to this database should be disabled or restricted.

Encryption of the data in the database cache is not recommended. The gateway message evaluation process requires frequent access to the messages in the database cache and encryption will impose performance overhead.

5. The message undergoes de-identification.

The clinical messages in the publication are de-identified using the privacy level specified in the topic. During this process, the anonymous ID that was assigned is inserted into the message, usually in place of other identifiers (note that this behavior could be modified by the implementation of the privacy level).

In our scenario in this Redbook, the messages are fully de-identified. The result is one or more HL7 messages with all the clinical information unchanged, but with no information relating to the patient identity.

The same HL7 could be included in more than one publication message. Each publication could have a different privacy level, as specified by the topic.

6. The publication message is produced.

At this point the message has been processed and the publication is ready to be sent to the broker for the matching topic. The publication should meet all the privacy level requirements and also have the capability to be re-identified should policy or legislation require such.

7. The publisher gateway passes the publication to the message flow server.

The HCN architecture is a hub-and-spoke configuration with the HCN Message Flow server as the hub. All gateways communicate with the hub using WebSphere MQ. The WebSphere MQ channels are encrypted using SSL to provide encryption, mutual authentication, and non-repudiation.

In a typical HCN installation, the gateways are owned by separate entities from the HCN Hub, and the connectivity between the gateways and the hub is through the Internet (or other public network). Firewalls are installed at each endpoint to prevent intrusion into the local networks. Each firewall should be configured to allow bi-directional communication between the two endpoints, using the port assigned to WebSphere MQ (by default, port 1414). WebSphere MQ uses this port for both control messages and data messages.

When the message is received at the Message Flow server, the WebSphere MQ process decrypts the message (using the private key assigned to the channel) and places it in the WebSphere MQ queue. Under normal operations, the WebSphere Business Integration Message Broker process (on which the HCN software is based) reads the message off the queue immediately, and through a hand-shaking process with WebSphere MQ, the message is deleted from the backing store (file system). This means that the clinical message appears unencrypted on the file system of the message flow server, if only for a brief time during normal operation. This implies that the Message Flow server itself must have strict access control to prevent unauthorized access to clinical messages while they are resident on the file system.

WebSphere MQ itself prevents unauthorized remote access to messages on its queues using SSL, through the mutual authentication feature. The public key for a remote client (any process that tries to access messages through WebSphere MQ) must be added to the key store of the Message Flow server queue manager for access to succeed. Any attempt to access the message

queues without using the SSL mutual authentication will be foiled by WebSphere MQ.

8. The publication is processed by the message flow server and sent to the subscriber gateway.

When the message flow server receives a publication message from the publisher gateway, it processes it and sends the message to the subscriber(s) that have been authorized to receive the topic. This process is the same as described in step 7 on page 178.

At this step in the flow, HCN enforces the publisher's right to authorize only specific subscribers to receive its data. The Message Flow server forwards HCN publications only to those subscribers who have been authorized by the publisher of this message for the topic identified by this message. In our scenario, only the ACN_SUBSCRIBER subscriber is authorized to receive messages for the topic *Influenza A* from the publisher *HOSPITAL_PUBLISHER1*.

Part of the subscription information maintained by the Message Flow server include the indication of whether the subscriber is to receive publications by e-mail or through a message to a subscriber gateway, or both. The flow described above is the path for sending the publication message to a subscriber gateway. The flow for the e-mail subscription option is described in step 10.

The Message Flow server also creates a log of all messages which are sent through the Message Flow server. Access to this log file must be strictly controlled.

9. The subscriber gateway makes the publication available in its environment.

On the Subscriber Gateway, the publication can be stored in the local DB2 database, sent to another application using the HCN HL7 connector, or some other customized action is performed on it. Each of these possibilities has security implications similar to those previously described. The server itself and any database must have access control implemented, and remote access to the database must be strictly controlled (if not disabled).

10. The message flow server talks to the Administrative server.

If the topic subscriber has requested the e-mail delivery option, the Message Flow Server sends the HCN Publication message to the HCN Administrative server over an encrypted SSL channel. Note that in a standard configuration, the Administrative server and Message Flow server would be in the same local network, and firewalls would not be required.

The Administrative server creates an e-mail addressed to the subscriber's designated recipient. This e-mail does not include the complete HL7 messages contained in the publication message, but only contains the summary information: the patient's anonymous ID, the topic name, the

publisher's name, and a time stamp. Nonetheless, in some circumstances, this information could be considered private and protected. It would be recommended in those cases that the Administrative server be configured to send encrypted e-mail using Public Key Encryption.

In addition, the Administrative Server and Message Flow Server can be configured to make a portion of the contents of the message flow server logs available to a publisher (containing only that portion of the log that was sent by that individual publisher). This process uses a daily script to transfer the partial log files to the Administrative Server via FTP. If publisher access to these partial log files is not required, you should disable the message log feature on the Message Flow Server.

6.5 Chapter summary

This chapter introduced the concepts of privacy and security in HCN and how HCN provides a secure electronic messaging system that is suitable for medical data.

Customizing Healthcare Collaborative Network

This appendix discusses how to customize Healthcare Collaborative Network. It begins with a discussion on how to extend Healthcare Collaborative Network by adding new connectors to integrate existing hospital applications more easily. It also discusses how to transform various local clinical codes that are used in different countries to the standard codes that are processed in Healthcare Collaborative Network by enhancing the transformation functions on the Gateway. Finally, this chapter discusses how to modify de-identification rules to meet the special privacy regulations applicable in your country.

This appendix includes the following sections:

- ▶ Preparing the HCN development environment
- ▶ Creating additional connectors
- ▶ Mapping local clinical codes
- ▶ Customizing HCN privacy rules
- ▶ De-identifying XML messages
- ▶ Consolidating HL7 messaging variation

Preparing the HCN development environment

To customize the Healthcare Collaborative Network (HCN) Gateway, you need the System Manager — an integrated development environment from the WebSphere Business Integration Toolset. You start by importing the Gateway artifacts from WebSphere Business Integration Server into the System Manager where you will make the changes and then redeploy the modified artifacts back to the WebSphere Business Integration Server.

The detailed steps are as follows:

1. Open the System Manager and change to the System Manager perspective of the Workbench.
2. From the InterChange Server Component view, right-click the InterChange Server Instance that is created by HCN and select **Connect** (Figure A-1). The default user ID is admin and the password is null.

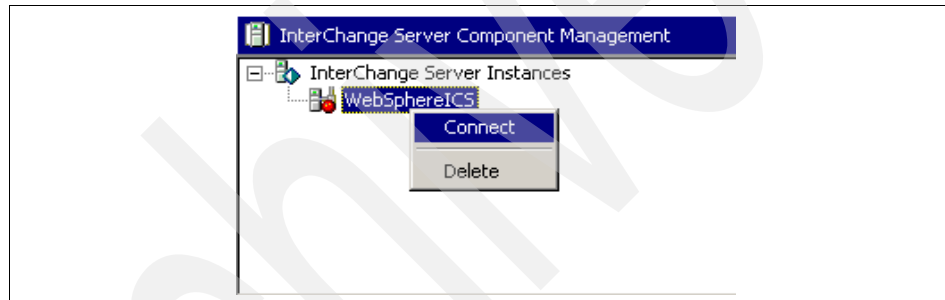


Figure A-1 InterChange server component manager

3. Right-click **Integration Component Library** in the upper left-hand pane of the Workbench and select **New Integration Component Library** (Figure A-2 on page 183).

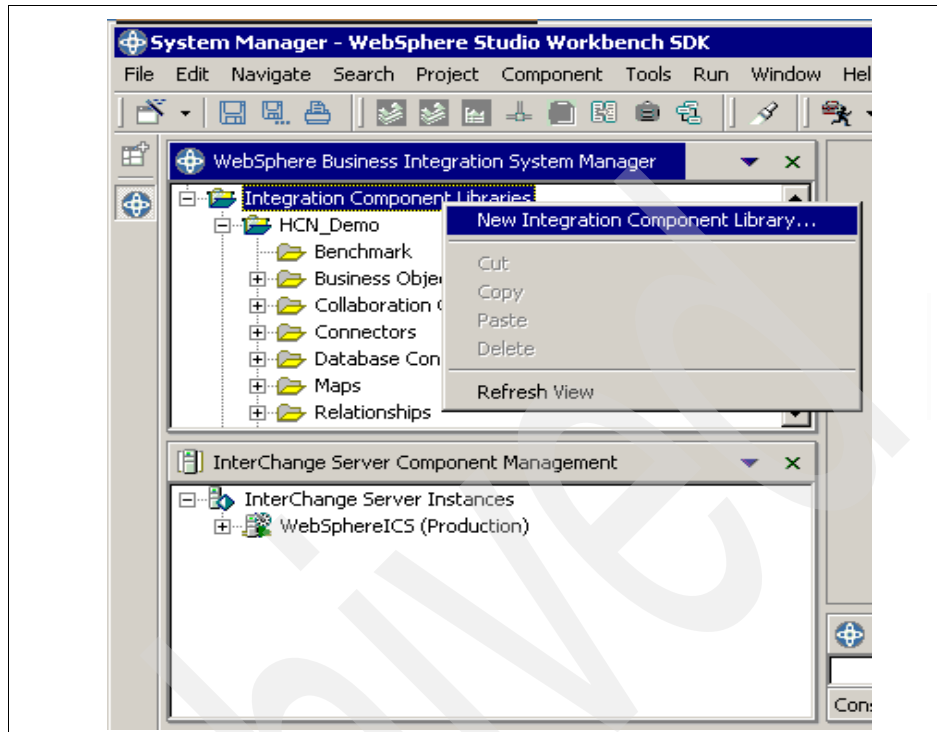


Figure A-2 Integration component library

4. Enter a name for your Integration Component Library project and select the appropriate instance of the HCN server from which you want to import. Click **Next** (Figure A-3 on page 184).

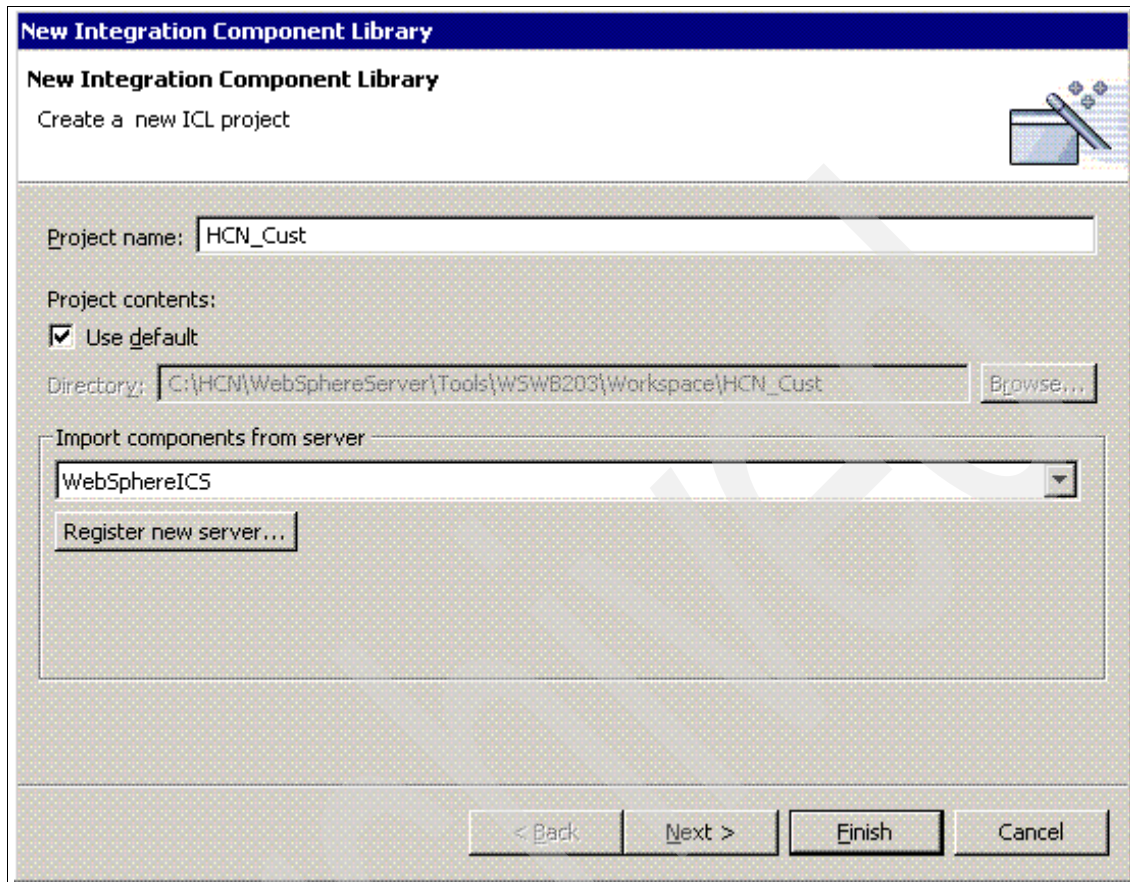


Figure A-3 Creating ICL project

5. Select the components that you want to import from the HCN server, and then click **Finish** (Figure A-4 on page 185). You should select all the components.

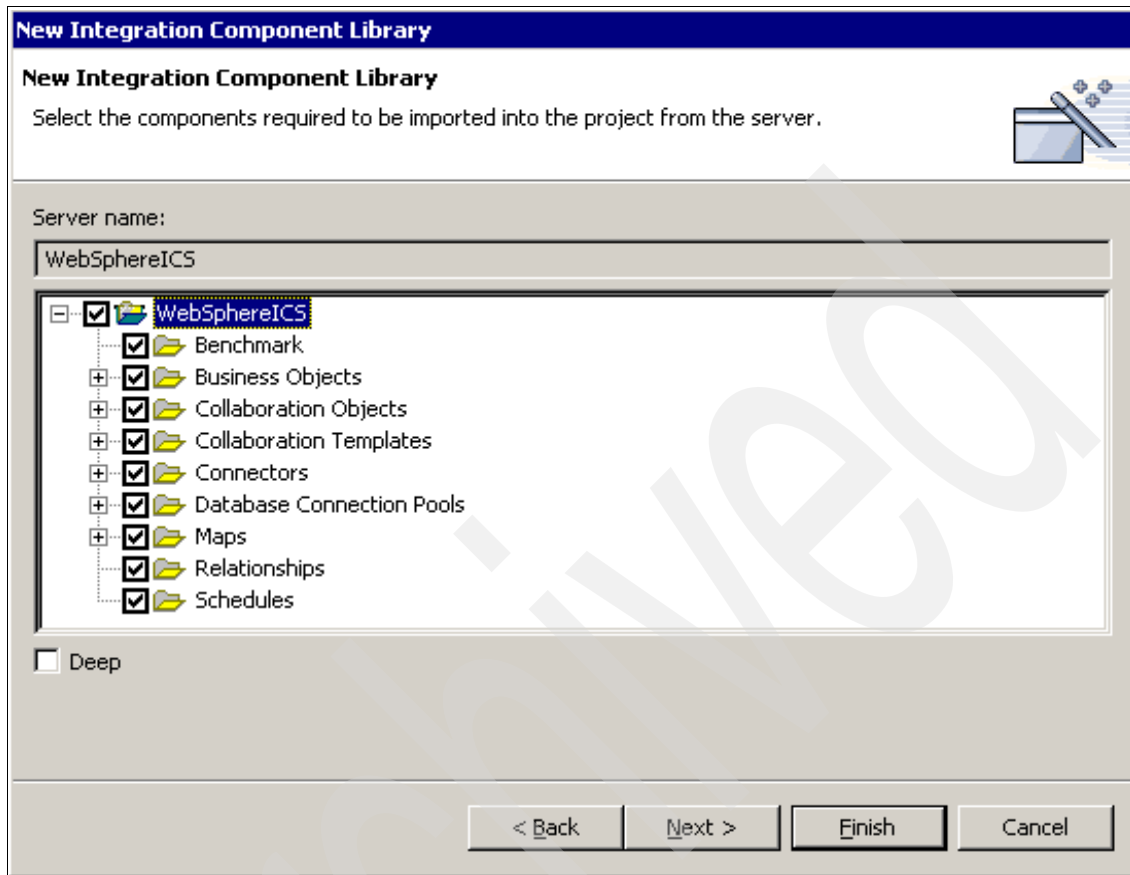


Figure A-4 Import required components

6. Expand and explore the newly created ICL project. All the components that HCN uses are grouped into eight different kinds of folders under this project. For our HCN customization, we will be modifying components in **Business Objects**, **Collaboration Objects** and **Connectors** folders. See Figure A-5 on page 186.

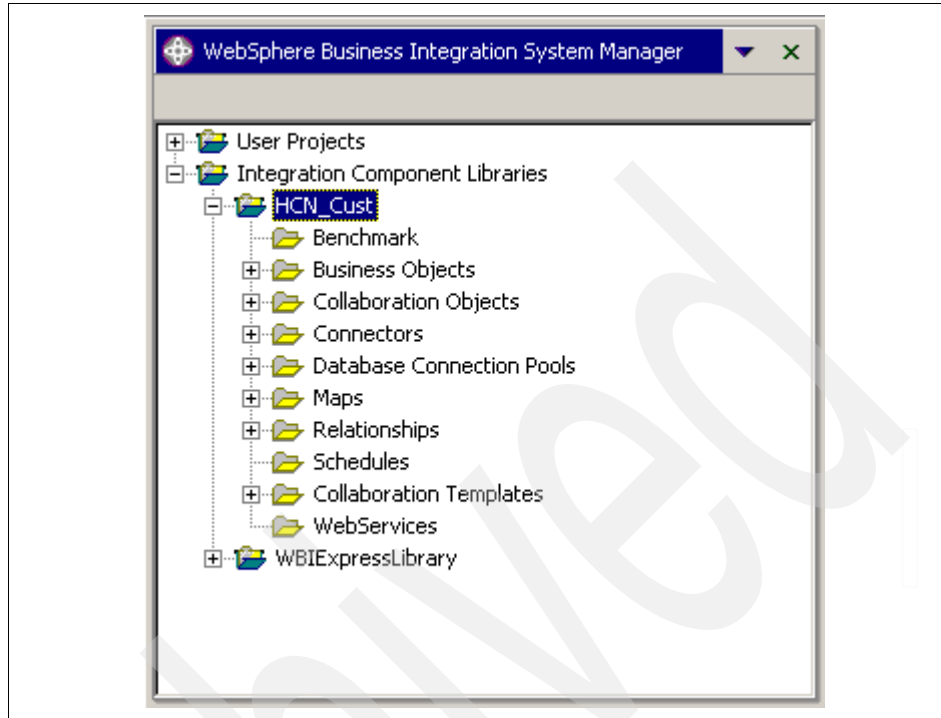


Figure A-5 Review the ICL components

You are now ready start your customization. You initiate modification of any of the components by performing one of the following:

- ▶ Double-click the component in the Connectors and Business Objects folder.
- ▶ Right-click the component in the Collaboration Objects folder and select **Properties**.

Note: You can use the WebSphere Business Integration Toolset for development without using the System manager. However, we describe only the steps for using the System Manager in our customization scenarios.

Note: The HCN development environment must be prepared only once, even if multiple customization steps are made later.

Creating additional connectors

The HCN product distribution includes five types of connectors to enable you to integrate your clinical information systems (CIS) applications with HCN. You can find these connectors in the <WBIS_Root>\connectors directory (see Figure A-6). Each type of connector uses a different transport or invocation method to integrate with existing applications.

Note: <WBIS_Root> refers to your installation directory for the WebSphere Business Integration Server. For example, if your WebSphere Business Integration Server is installed in the C:\HCN\WebSphereServer directory, then <WBIS_Root> refers to C:\HCN\WebSphereServer.

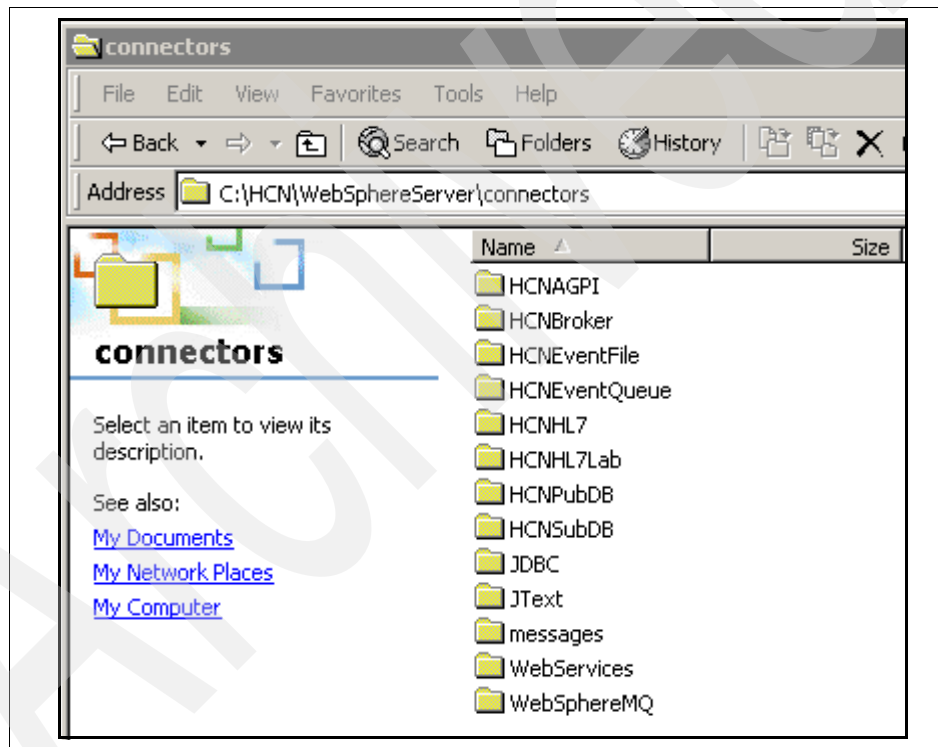


Figure A-6 HCN connectors

The following are the HCN default connectors:

► **JDBC Connector**

This type of connector supports exchanging of data with applications through database access. Both the publisher gateway and subscriber gateway include a JDBC connector that is used to access the internal HCN Gateway database (named HCNPubDB and HCNSubDB, respectively). A customized version of the JDBC connector could be used to integrate with a CIS application.

► **Health Level 7 (HL7) LLP Connector**

The HL7 LLP connector supports the exchange of HL7 messages through the HL7 Mixed Low-level Protocol (MLLP), which is a TCP/IP-based protocol. This connector, named HCNHL7, can be used to exchange HL7 clinical messages with CIS applications. Additional copies of this connector can be made to support data exchange with multiple CIS applications. Although the MLLP protocol could be used to exchange messages other than HL7 messages, in practice this is rarely done.

► **JText Connector**

This type of connector supports exchanging of data through file sharing or FTP. HCN Gateway installation creates a JText connector named HCNEventFile for file message exchange from a specified directory.

► **WebSphereMQ Connector**

The WebSphereMQ connector supports exchanging of data between HCN and applications through the use of WebSphere MQ queues. HCN includes two WebSphereMQ connectors. The connector named HCNBroker is used for sending and receiving messages between the HCN Gateway and the HCN Message Flow Server. The connector named HCNEventQueue is provided to allow the exchange of HL7 or XML messages with a CIS via WebSphere MQ queues.

► **WebServices Connector**

This type of connector supports exchanging of data using WebServices protocols (SOAP over HTTP or SOAP over JMS). A WebServices connector named HCNAGPI is included in the HCN Gateway to invoke AGPI services. A customized version of the WebServices connector could be used to exchange clinical messages with a CIS application.

The HCN Publisher Gateway provides two ports through which a connector can send messages into the gateway. These two ports are named InputHL7Messages and InputXMLMessages. These names, however, are misleading because either port can be used to receive XML messages or HL7 messages.

By default, the InputHL7Messages port is bound to the HCNHL7 connector, meaning that messages from the HCNHL7 connector are sent to the publisher gateway for evaluation. The InputXMLMessages port is bound to the HCNEventFile connector. So using the default configuration, messages can be received through one HL7 MLLP application and from one file-based application. This means that the HCNEventQueue connector is not bound to any port, and does not send messages to the publisher gateway. Steps 17 on page 196 through 24 on page 199 describe how to modify the bindings to change which connectors send data to these two ports. You can follow these steps to change the bindings to use an existing connector.

In our customization scenario, you learn how to create additional connectors. We create an additional HL7 MLLP connector which uses the TCP/IP-based MLLP to exchange HL7 messages.

To create a new HL7 MLLP connector, you need to perform the following steps (You should have prepared your development prior to creating connectors, as described in “Preparing the HCN development environment” on page 182):

1. In the <WBIS_Root>\Connectors directory, duplicate the HCNHL7 folder.
2. Change the duplicate folder name to the desired and unique name of your new connector (Figure A-7).

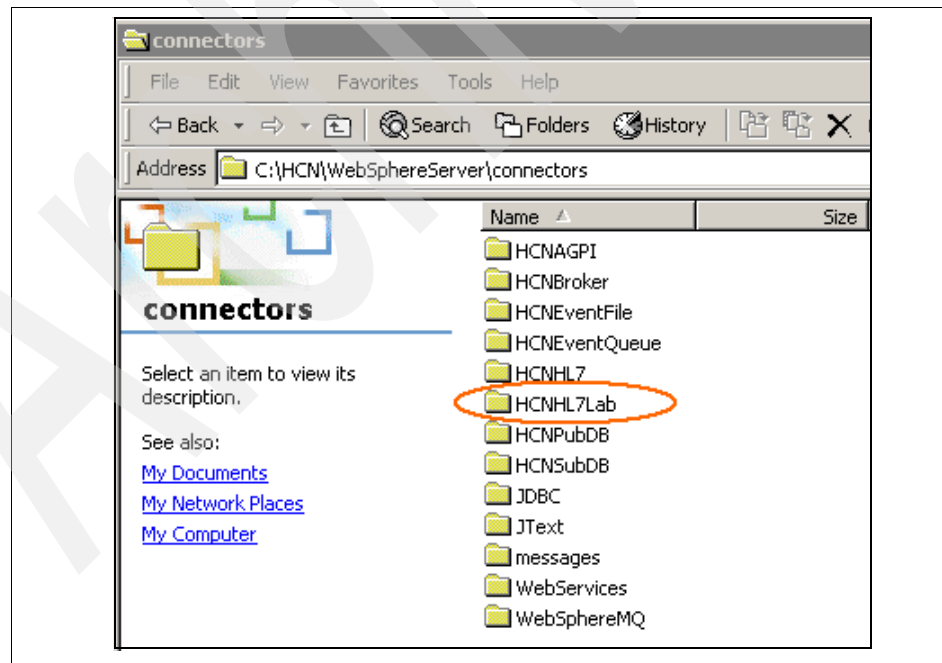


Figure A-7 Creating new HCN connector

3. Copy the HL7 connector shortcut on your desktop.
4. Paste a copy of the shortcut onto your desktop and rename it (Figure A-8 on page 190).

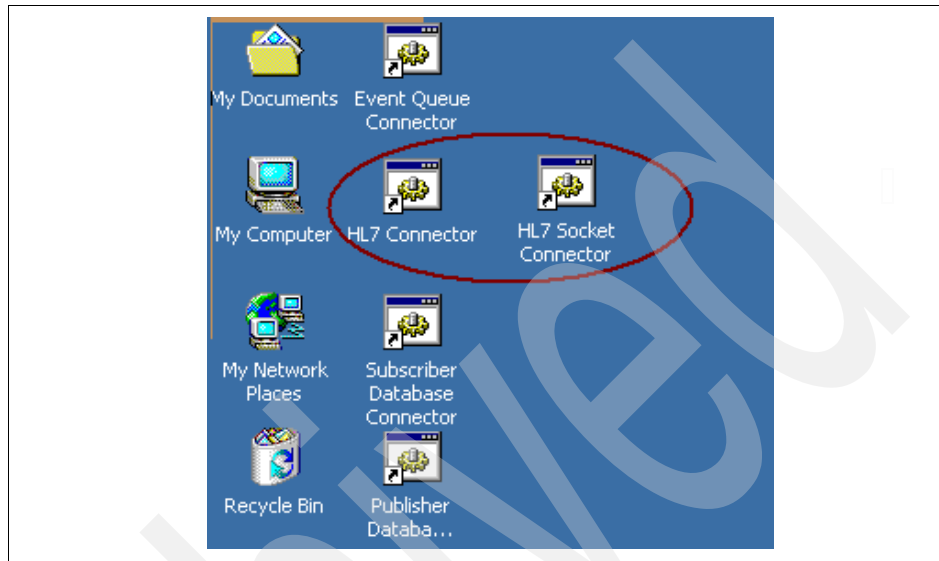


Figure A-8 Creating shortcut for new connector

5. Open the new shortcut's properties (ensure that the Shortcut tab is selected).
6. In the path segment of the Target field, change the reference to HCNHL7 to the unique name of your new connector from step 2 on page 182. (For example, we used HCNHL7Lab in this scenario.)
7. In the first parameter segment of the Target field, also change the reference to HCNHL7 to the unique name of your new connector from step 2 on page 182.

For example, you would change the following:

`<WBIS_Root>\connectors\HCNHL7\start_HL7.bat HCNHL7 WebSphereICS`

To this:

`<WBIS_Root>\connectors\HCNHL7Lab\start_HL7.bat HCNHL7Lab
WebSphereICS`

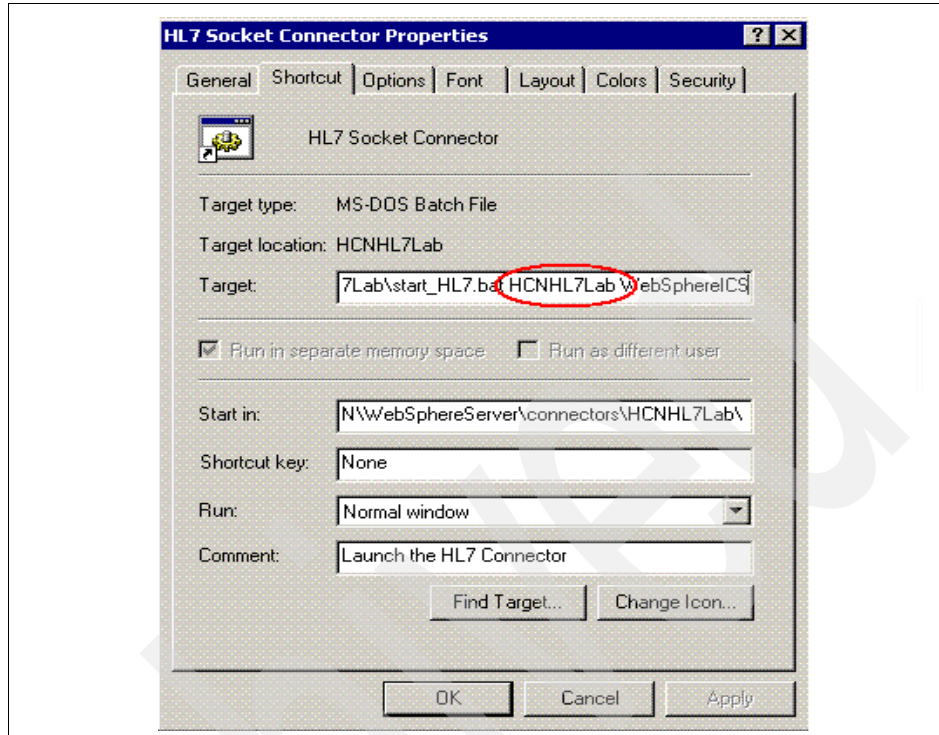


Figure A-9 Modify target of shortcut for new connector

8. Open the start_HL7.bat in the file directory for your new connector (see the path in step 7 on page 190).
9. Modify the AGENT variable with new path such that it points to the newly created connector. For example, change the following:

AGENT="%CROSSWORLDS%\connectors\HCNHL7\CWHL7.jar

To this:

AGENT="%CROSSWORLDS%\connectors\HCNHL7Lab\CWHL7.jar

```

rem @echo off
call "%CROSSWORLDS%\bin\CWConnEnv
setlocal

REM set the directory where the specific connector resides
set CONNDIR="%CROSSWORLDS%\connectors\%1

REM goto the connector specific drive & directory
cd /d %CONNDIR%

REM set the name to be the application connector that is starting
set CONNAME=%1

REM set the server name to be the interchange that is being targeted
set SERVER=%2

set AGENT="%CROSSWORLDS%\connectors\HCNHL7Lab\CWHL7.jar
set JCLASSES=%JCLASSES%;%AGENT%

REM config file location defaults to HOME\Interchangesystem.cfg on th

REM start the Java connector under the Java Application End
rem %CWJAVA% -oss10m -mx128m -Djava.library.path="%CROSSWORLDS%\bin;
%CWJAVA% -oss10m -ms64m -mx128m %ORB_PROPERTY% -Djava.ext.dirs="%MQ_L
endlocal

```

Figure A-10 Modify .bat file for new connector

10. Open WebSphere MQ Explorer and create a local queue under WebSphere Business Integration Server queue manager for communication between new connector and WebSphere Business Integration Server.
11. Give the queue name an AP or unique name that is concatenated with CONNECTOR/WEBSPHERICCS. For example
AP/HCNHL7LABCONNECTOR/WEBSPHERICCS (Figure A-11 on page 193).

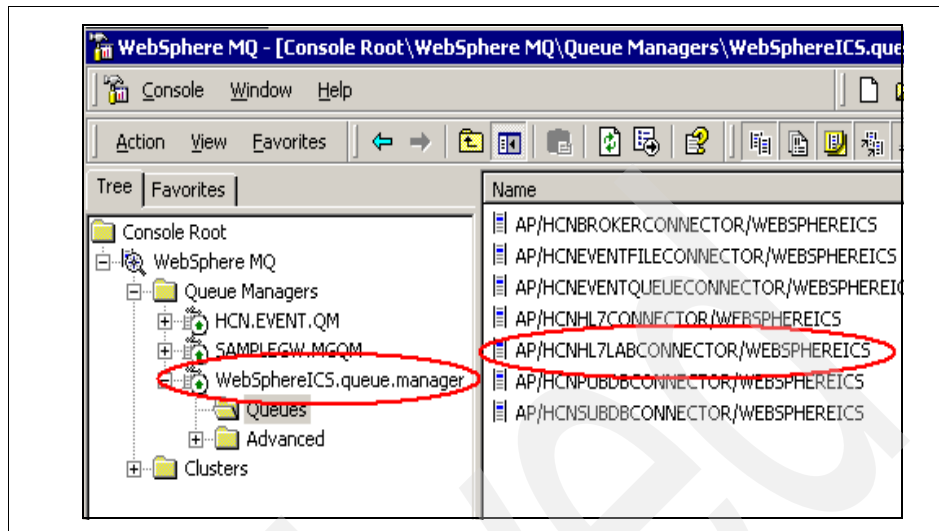


Figure A-11 Creating queue for connector

12. Double-click the HCNHL7 connector in the System Manager to open the connector configurator
13. On the Standard Properties tab, modify the application name property to be your unique name concatenated with the word Connector. For example, our customization scenario is HCNHL7LabConnector.

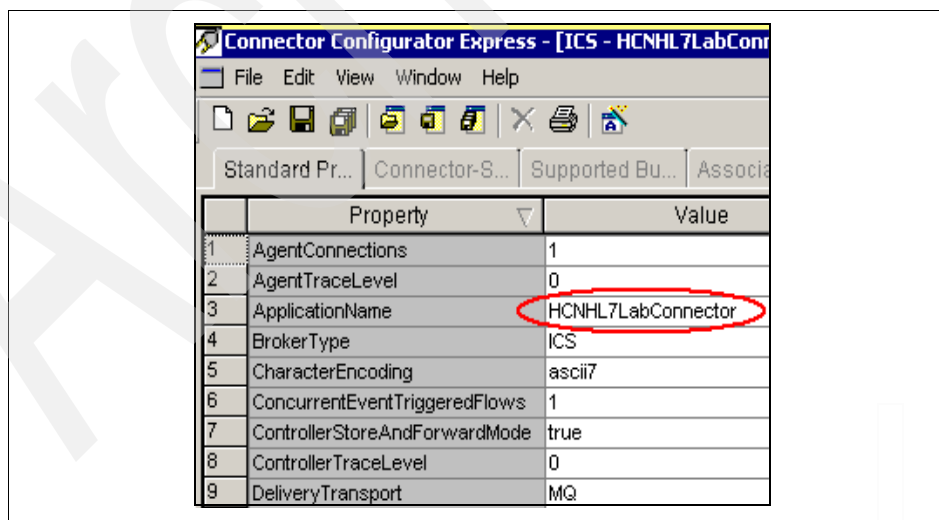


Figure A-12 Modify the properties for new connector

16. Give the connector a unique name that is concatenated with Connector, for example, HCNHL7LabConnector. Ensure that the project that you created to hold the HCN artifacts is selected in the Project drop-down.

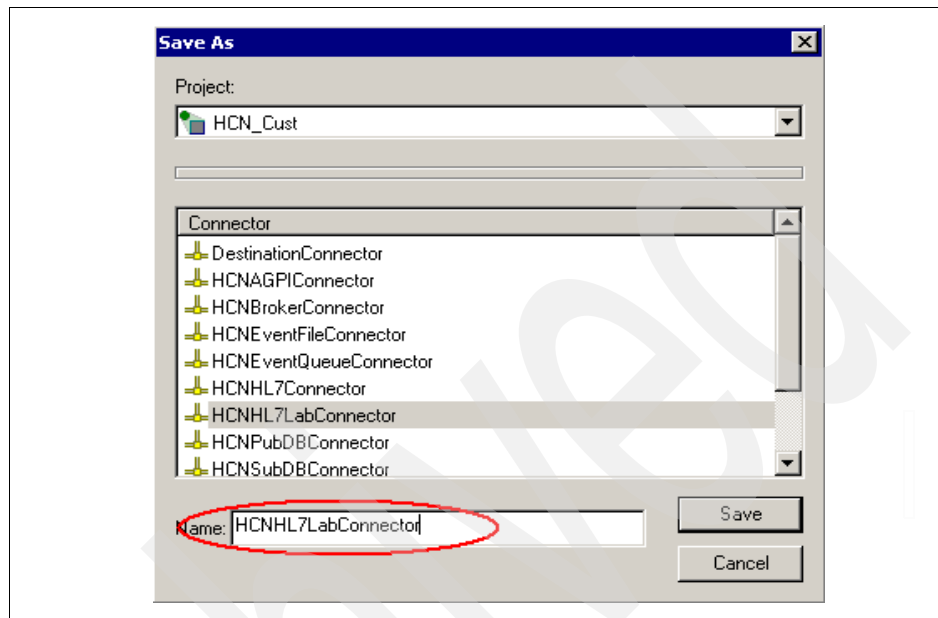


Figure A-15 Creating new connector component in ICL project

Tip: It is advisable to ensure that your default Log file and Trace file sizes are set to something greater than zero (0) before you save the new connector component. Otherwise, you will not be able to save your connector (Figure A-16).

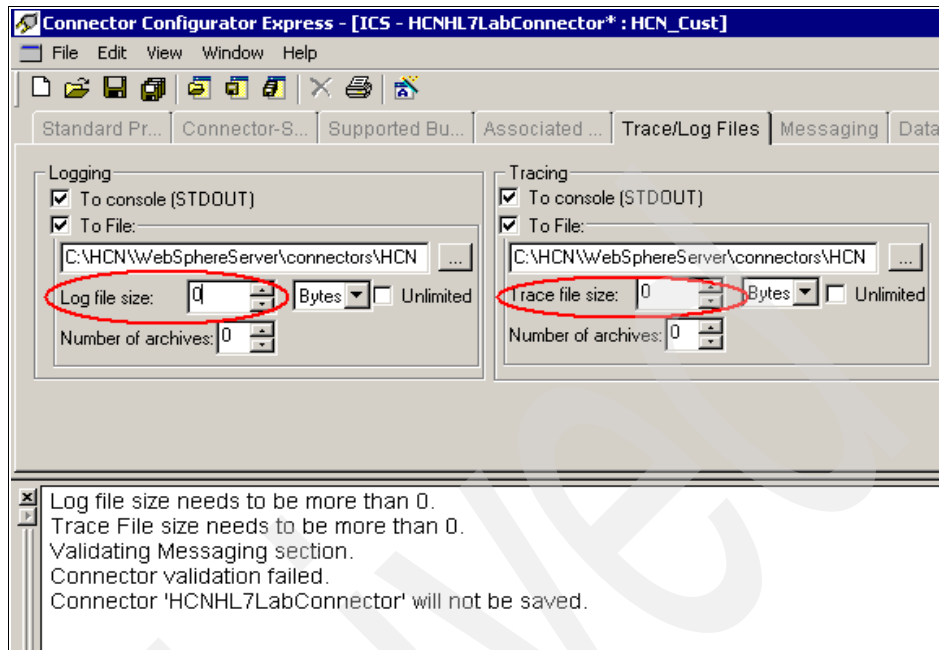


Figure A-16 Enable trace for connector

17. Double-click the Hospital_To_Gateway_Entry::HCN_Entry collaboration object under the ICL project that you prepared before, and then select the tree view to modify the port binding of this collaboration.
18. Choose which port you want to bind the new connector to. In this example, we bind our new connector to the InputHL7Messages port of Hospital_To_Gateway_Entry::HCN_Entry collaboration.
Right-click the desired port and click **Bind Port** (Figure A-17 on page 197).

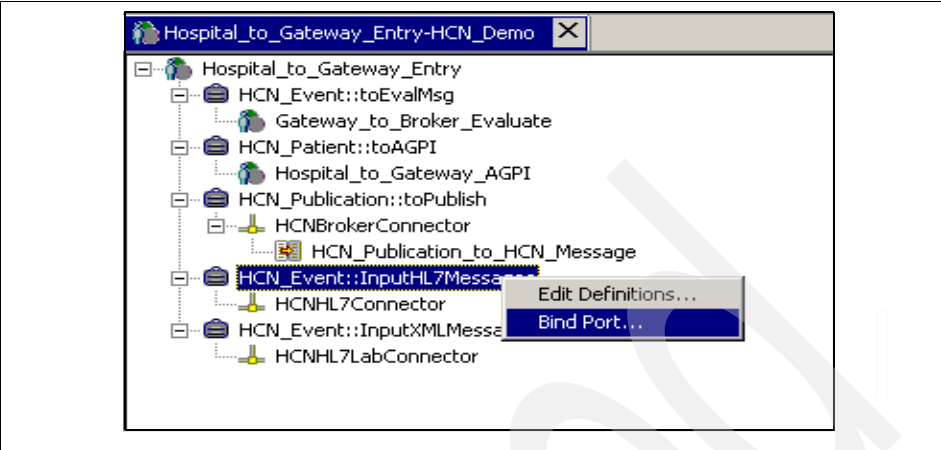


Figure A-17 Bind connector to a port

19.Choose your new connector and click **OK**.

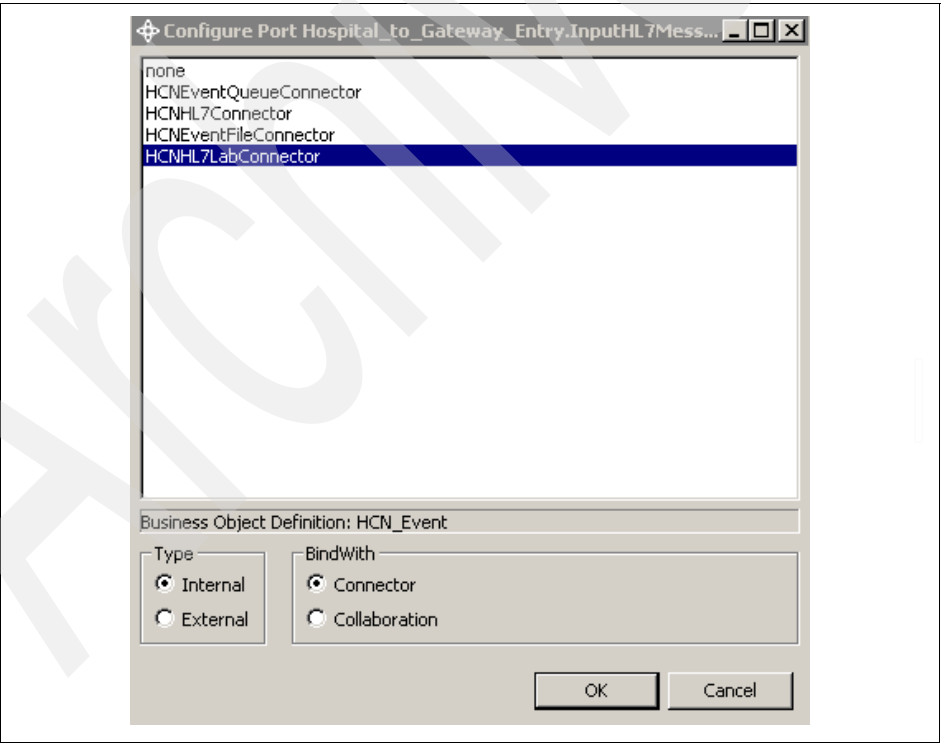


Figure A-18 Bind new connector to Port

20. From the InterChange Server Component Manager view in System Manager perspective, right-click the Hospital_to_Gateway_Entry::HCN_Entry collaboration object (which must be replaced) and select **Stop**.

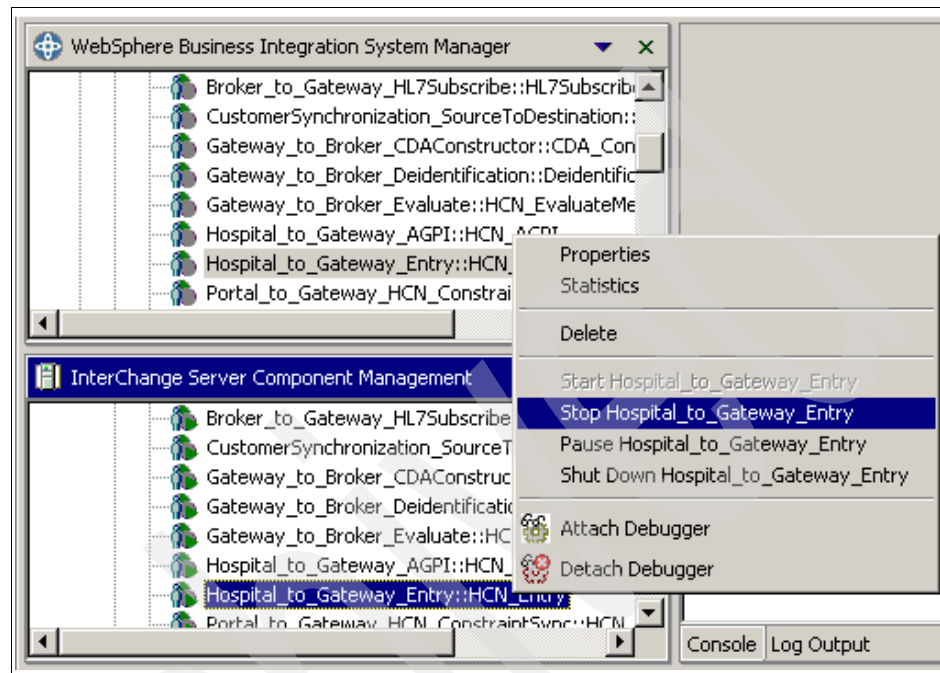


Figure A-19 Stop collaboration object

Note: Several of the collaborations are linked together through their input and output ports. The ICS server stops all of the collaborations when one is stopped and starts them all when one is started.

21. Click the Hospital_to_Gateway_Entry::HCN_Entry collaboration object in the Collaboration Objects folder of the ICL project in InterChange Server Component view. Drag it down to the same folder in the InterChange Server Component view (Figure A-20 on page 199).

Tip: When dragging objects in the System Manager, you must press and hold mouse button 1, rather than mouse button 2, as when dragging and dropping in Windows.

22. Click your new connector object in the Connectors folder of the ICL project in InterChange Server Component view, and drag it down to the same folder in the InterChange Server Component view.

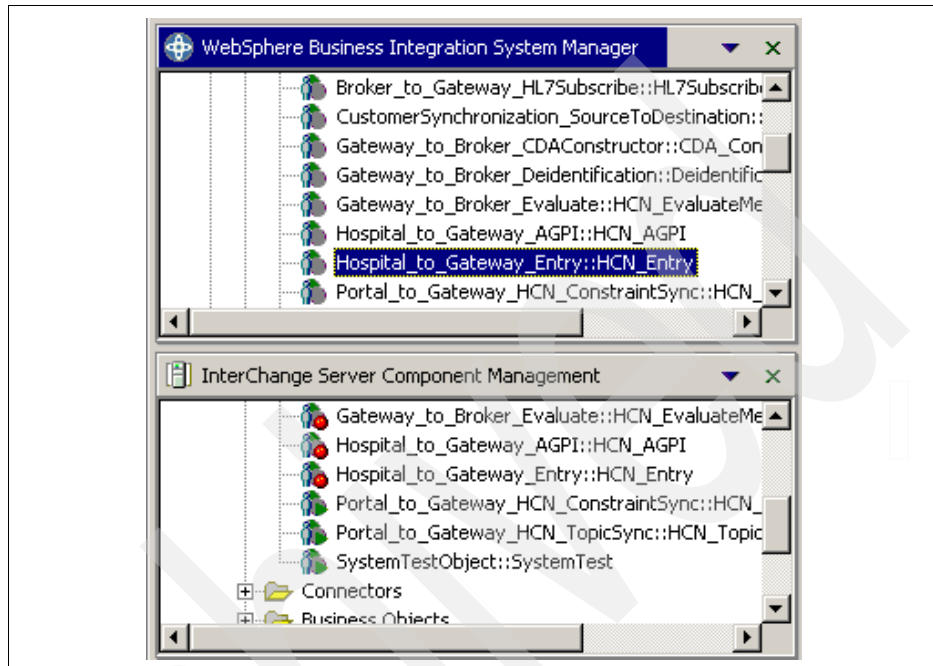


Figure A-20 Deploy collaboration object.

23. Restart the InterChange Server.
24. Start the Hospital_to_Gateway_Entry::HCN_Entry collaboration object under the InterChange Server Component view. Ensure that all collaboration objects and connectors are started.

Note: If you need to modify the Collaboration Object properties after deployment, you must do so in the Integration Component Libraries and redeploy it to the InterChange Server instances created by HCN as described prior. You cannot change properties directly under InterChange Server Instance.

You are now ready to test your new connector. We use the HL7 Simulator application from INTERFACEWARE for testing. HL7 Simulator simulates a CIS application which communicates with your newly created connector through a TCP/IP socket.

25. Open HL7 Simulator application (Figure A-21 on page 200).

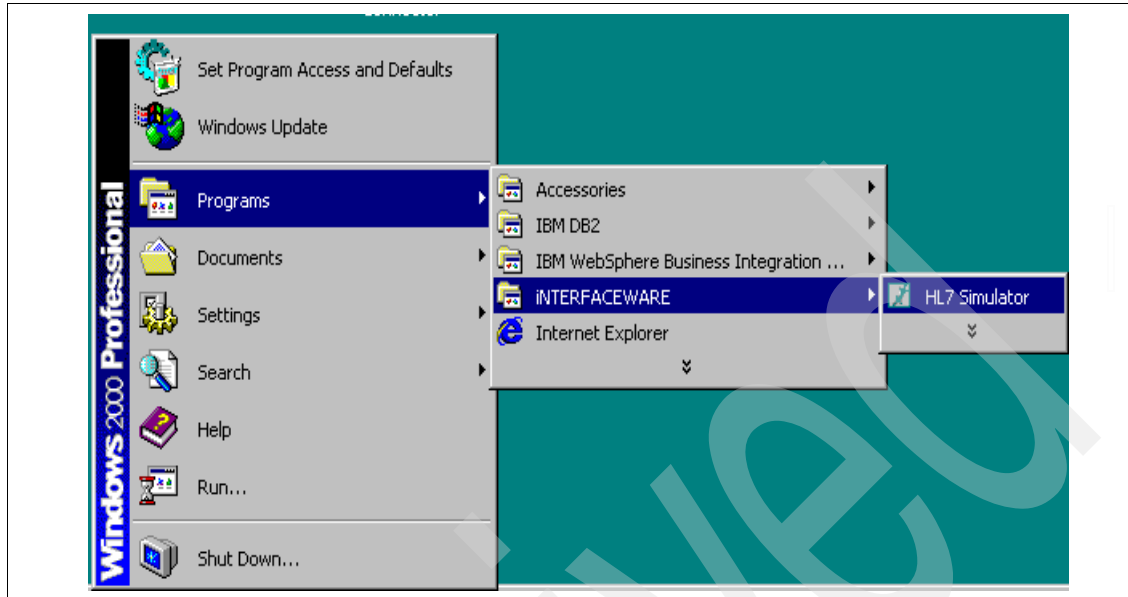


Figure A-21 HL7 simulator

26. Input the host name and the listening port of the connector. The listening port is the Server Port property of the HCNHL7Lab connector. Choose the message file that contains the HL7 evaluation messages.
27. Select **Keep sending messages when ACK Received?** and **Stop sending messages at end of file?** and click **Start** to start send test HL7 messages to your new connector (Figure A-22 on page 201).

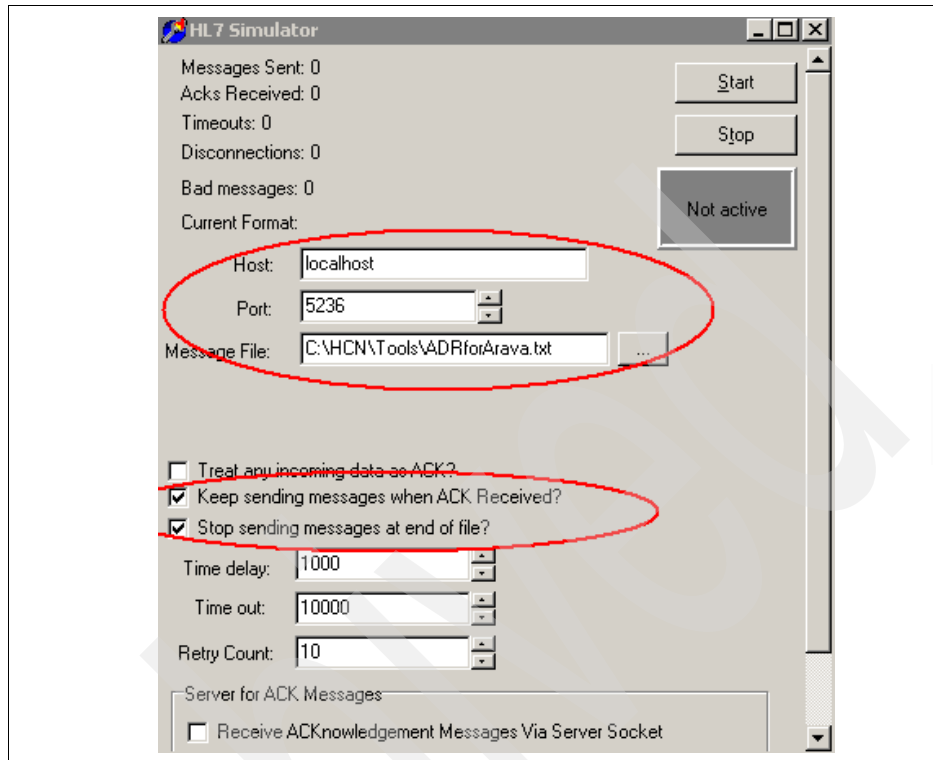


Figure A-22 Chameleon HL7 testing simulator

28. Open the System View of System Manager to monitor the state of connectors. Notice that the number for Message Sent in the HL7 simulator should match the number of messages that were processed by your connector (Note that this is displayed in the Total Sent column in the System View in Figure A-23 on page 202).

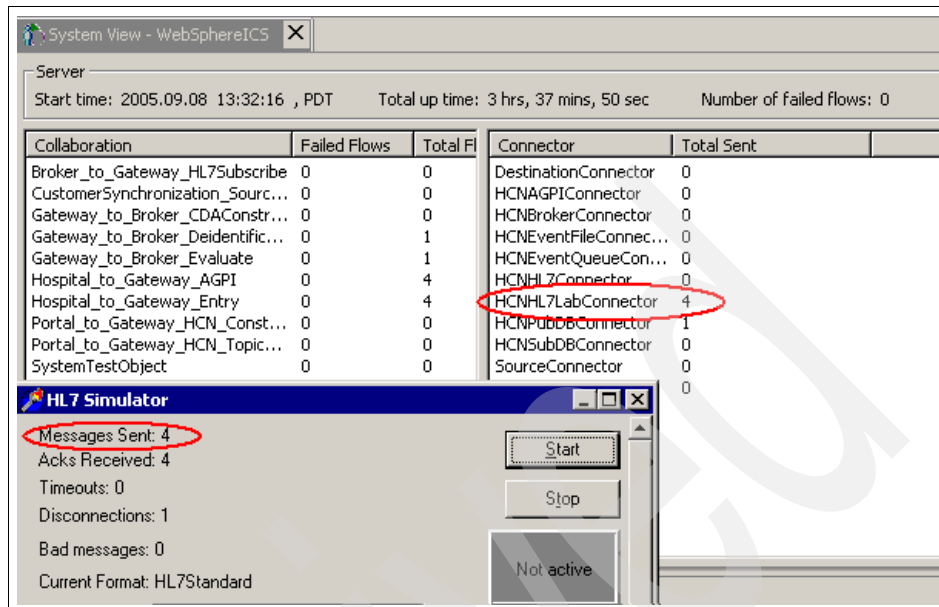


Figure A-23 Testing new connector

To conclude this section on how to create additional connectors, we summarize the steps for creating new connectors. Although there are many reasons for wanting to create new connectors, the safest means for creating a new connector is to start with any of the HCN supplied connectors. The following are the steps for creating additional connectors:

- ▶ Duplicate the directory for the kind of connector you want to create.
- ▶ Rename the directory to your chosen name for the connector.
- ▶ Create a shortcut for the new connector and change the Target property field appropriately.
- ▶ Modify the .bat file to set the appropriate environment variables for the new connector.
- ▶ Add a new queue in WebSphere Business Integration Server queue to manage the communication between connector and WebSphere Business Integration Server.
- ▶ Create a new connector component in Integration Component Library.
- ▶ Configure the new connector using Connector Configurator tool.
- ▶ Bind the new connector to the proper port by modifying Hospital_To_Gateway_Entry collaboration object.

- Deploy all collaboration objects and connectors modified to WebSphere Business Integration Server.

Mapping local clinical codes

Open standards are necessary for successful collaborative exchange and interpretation of healthcare data involving large groups of participants. HCN is designed to process HL7 version 2.4 messages. The HL7 standard does not include, nor does it enforce, a common data dictionary. HCN processes HL7 messages, which are defined using the following industry accepted coding standards:

- Logical Observation Identifiers and Codes (LOINC) for laboratory results.
- International Classification of Disease codes, version 9 (ICD-9) for diagnoses.
- Current Procedural Terminology (CPT4) or ICD-9 for clinical procedures.

HCN mapping capabilities facilitate the transformation of your data to meet the standard vocabularies. As an example, we demonstrate how to replace local laboratory codes within the HL7 messages with LOINC code. By following the steps in this example, you should be able to map other types of codes. The steps include the following:

1. Enable external mapping capability of HCN Gateway first. To do this, you need to set the `TRANSLATION` property in the `Hospital_To_Gateway_Entry` collaboration to `TRUE` and make the `TRANSLATION_VMD` property in the `Hospital_To_Gateway_Entry` collaboration point to the external Chameleon mapping module. As a reference, HCN Gateway ships with a sample module for transforming local laboratory code to LOINC code. This module is named `OBXCodeMapping.vmd` and is found in the `<PublisherGateway_Root>\vmd\` directory.
2. Create a database table to define the mapping rules between local coding system and standard coding system. In our scenario, we choose IBM DB2 to store mapping tables used for mapping local laboratory code to LOINC code. You can find the Data Definition Language (DDL) file for our scenario in the `<PublisherGateway_Root>\db` directory. Type the commands in Example A-1 from the DB2 command window to create the database for holding the mapping tables.

Example: A-1 DB Script for code mapping

```
C:\HCN\Gateway\Publisher Gateway\db>db2 connect to HCNPUB
```

```
Database Connection Information
```

```
Database server          = DB2/NT 8.1.5
```

```
SQL authorization ID    = ADMIN
Local database alias    = HCNPUB
```

```
C:\HCN\Gateway\Publisher Gateway\db>db2 -f observationcodes.sql
DB20000I The SQL command completed successfully.
```

```
DB20000I The SQL command completed successfully.
```

```
C:\HCN\Gateway\Publisher Gateway\db>db2 insert into observationcodes
values('wc','L','15061-5','LOINC','')
DB20000I The SQL command completed successfully.
```

Note: The script creates a table with five columns. LOCALCODE and LOCALCODESET columns are used for the local vocabulary, columns STANDARDCODE and STANDARDCODESET are the corresponding standard vocabulary, and the fifth column is used for a description of the term. In this example, mapping local vocabulary to the standard vocabulary is a table look-up process where the local code and local code set are used to find the corresponding standard code and code set. For example, local laboratory code named wc of local coding system L maps to standard LOINC code and value of 15061-5. More complex logic than a simple table look-up might be necessary for certain kinds of mapping. This topic that is beyond the scope of this book.

3. Open mapping module file OBXCodeMapping.vmd.
4. Open the inbound equation editor window by selecting **Chameleon** → **Inbound equation**.
5. Enter the following command:

```
import dbconn
```

Note: For Chameleon to access the database tables that we created, you need to establish a database connection. You establish the connection using the Python script that you just imported. Chameleon looks for the Python script (in our example the name of the script file is dbconn.py) in the directory that is defined in the CHM_PYTHON_LIB_PATH environment variable.

In Example A-2, the Python script dbconn.py establishes the connection using the ODBC database connection to HCNPUB ODBC data source, which is configured in a Windows system. Specifying the user name and password in the script file (as is shown in the example) is the only method of specifying connection information that is supported by the ODBC module of the Python Windows Extension project that we use in this scenario. Because the statement that opens the database connection is not contained within a function definition in the dbconn.py script, it is executed only once by the Python runtime — the first time the script is imported. In this manner, the database connection is opened once and reused every time the mapping function is invoked.

Example: A-2 Python script for DB connection

```
*****
#* OCO Source Materials *
#* Package: com.ibm.hcn.* *
#* * *
#* (C) Copyright IBM Corporation 2003 *
#* The source code for this program is not published or otherwise *
#* divested of its trade secrets, irrespective of what has been *
#* deposited with the US Copyright Office. *
#*****
import dbi,odbc

# open a database connection
dbc = odbc.odbc ('HCNPUB/admin/password')
```

6. For each HL7 message, select **Segment grammar**.
7. Click **Message Function** to open the pass-through mapping code (Figure A-24 on page 206).

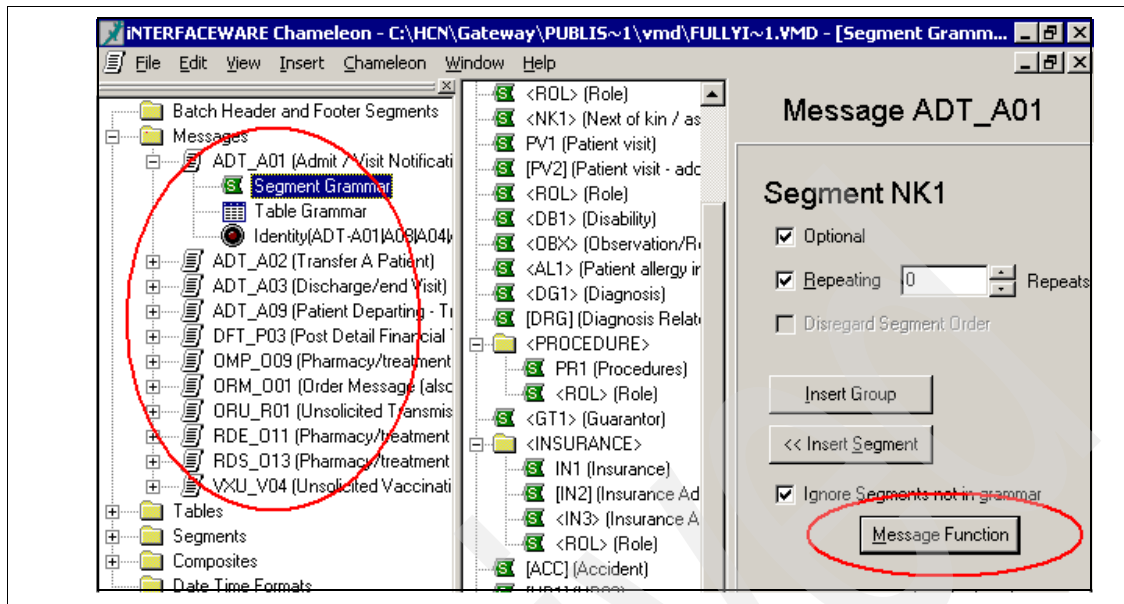


Figure A-24 Segment grammar

Note: The message function code in Example A-3 shows an example of mapping local laboratory code to LOINC code. This example processes only OBX segments (that is, the observation result field) in the HL7 message. The sample code shows that we pick up the values from the Identifier and Name of Coding System subfields, which are the first and third subfields of the Observation Identifier field (Observation Identifier is the third field, in the OBX segment). We then search the mapping table that we defined in the database to find the corresponding LOINC code. Finally, we replace the values in the Identifier and Name of Coding System fields with the corresponding LOINC code and LOINC code set. The prior values are moved to the Alternate Identifier and Name Of Alternate Coding System fields for tracking purposes.

Example: A-3 Python sample script for code mapping

```
# database connection (dbconn.dbc) is imported in the inbound equation
result=" "
crsr=None

# Get an iterator that points to the first segment
iterator = environment.input_segment_iterator()
output = iterator.output()
```

```

#Repeating loop OBX
while iterator.move_one():
    if iterator.segment_id() == 'OBX':
        if crsr == None:
            # create a cursor
            crsr = dbconn.dbc.cursor ()

            # search for the local observation code in the database
            sql1 = "SELECT * FROM ObservationCodes where LocalCodeSet='"
            LocalCodeSet = iterator.field(3).subfield(2).value
            sql1 = sql1+ LocalCodeSet + "'"
            LocalCode = iterator.field(3).subfield(0).value
            sql1 = sql1 + " and LocalCode='"+LocalCode+"'"
            rc = crsr.execute(sql1)
            result=crsr.fetchone()

            if result!=None:
                Atext=iterator.field(3).subfield(1).value
                iterator.field(3).subfield(0).value=result[2]
                iterator.field(3).subfield(1).value=result[4]
                iterator.field(3).subfield(2).value=result[3]
                iterator.field(3).subfield(3).value=LocalCode
                iterator.field(3).subfield(4).value=Atext
                iterator.field(3).subfield(5).value=LocalCodeSet

        output = output + iterator.output()

value=output

if crsr!=None:
    # close the cursor
    crsr.close()
    crsr = None

```

Modifying or extending the predefined codesets

The HCN Administration server includes database tables that contain reference codes or terms in four clinical areas: observations, diagnoses, procedures, and drugs. The reference terms that HCN provides are:

- ▶ LOINC: August 2002 version of LOINC from:
<http://www.regenstrief.org/loinc/>
- ▶ ICD-9 CM: 2003 version of ICD-9 CM
- ▶ Drug names: Drug database from Health Canada, 2003
- ▶ ICD-9 procedures plus CPT-4 procedures

These reference terms represent the standards that are selected by IBM for each of these domains. When creating topics in the HCN Administration application, HCN validates the user input for lab result codes, diagnosis codes, and drug names against these tables and accepts only values that are found in the database table.

A joke heard frequently at Healthcare standards meetings is that the great thing about standards is there are so many to choose from. The standard reference terms that are selected by IBM might not be the ones that are chosen for use in any particular HCN installation.

To modify the predefined codesets for observations, diagnoses, or drug names, follow the steps in one or more of the sections that follow. Of course, there are a wide variety of DB2 commands, SQL, command-line tools, and programs that you can use to manipulate data files and to load the contents into a DB2 database. What we present here is one possible method of modifying the content of these tables.

These instructions assume that you are logged onto the HCN Administrative Server with the same user ID that performed the HCN Administrative Server installation.

Drugs

The predefined data for the Drug database are contained in the following file:

```
<HCN_Admin_Server_Install_Root>\database\setup\data\topic\drugs.txt
```

There are only two fields in the drug table — an automatically generated ID and the Name column that contains the name of the drug. Therefore, the file that contains the drug names has no delimiters. Each line contains the full name of the drug.

To replace the pre-installed drug table with a different set of drug names, first create or acquire a file that contains the drug names. For this example, we assume the file is:

```
<HCN_Admin_Server_Install_Root>\database\setup\data\topic\mydrugs.txt
```


Open a DB2 command window and issue the commands that are shown in Example A-4.

Example: A-4 Replacing the pre-installed drug table

```
db2 connect to HCN_DB
db2 drop table ADMIN.Drug
cd "<HCN_Install_Root>\Administrative Server\database"
db2 -td; -f.\db\topic\user\drug.sql
db2 load from .\setup\data\topic\mydrugs.txt of del insert into ADMIN.Drug
(Name)
db2 connect reset
```

Procedures

The predefined data for procedure codes are found in these two files in the <HCN_Admin_Server_Install_Root>\database\setup\data\topic\ directory:

- ▶ icd9_procedure_codes.txt
- ▶ cpt4_procedure_codes.txt

The format of these files is that each line contains a procedure code and a procedure name or description that is separated by a vertical bar (or pipe, "|") delimiter. The database table itself contains a generated ID column plus these two fields. The generated ID column is accounted for by using the modified by identitymissing clause on the DB2 **load** command.

To replace the pre-installed procedure table with a different set of procedure codes, first create or acquire a file that contains the procedure codes in this format. For this example, we assume the file is:

```
<HCN_Admin_Server_Install_Root>\database\setup\data\topic\
myprocedures.txt
```

Open a DB2 command window and issue the commands that are shown in Example A-5.

Example: A-5 Replacing the pre-installed procedure table

```
db2 connect to HCN_DB
db2 drop table ProcedureCode
cd <HCN_Install_Root>\Administrative Server\database
db2 -td; -f.\db\topic\user\procedure_code.sql
db2 "load from .\setup\data\topic\myprocedures.txt of del modified by
coldel| identitymissing insert into ProcedureCode"
db2 connect reset
```

Diagnoses

The predefined data for diagnosis codes are contained in the following file in the <HCN_Admin_Server_Install_Root>\database\setup\data\topic directory:

icd9_diagnosis_codes.txt

The format of this file is that each line contains a diagnosis code and a diagnosis name or description that is separated by a vertical bar (or pipe, “|”) delimiter. The database table itself contains a generated ID column plus these two fields. The generated ID column is accounted for by using the modified by identitymissing clause on the DB2 **load** command.

To replace the pre-installed diagnosis table with a different set of procedure codes, first create or acquire a file that contains the diagnosis codes in this format. For this example, we assume the file is:

<HCN_Admin_Server_Install_Root>\database\setup\data\topic\
mydiagnoses.txt

Open a DB2 command window and issue the commands that are shown in Example A-6.

Example: A-6 Replacing the pre-installed diagnosis table

```
db2 connect to HCN_DB
db2 drop table DiseaseDiagnosisCode
cd <HCN_Install_Root>\Administrative Server\database
db2 -td; -f.\db\topic\user\disease_diagnosis_code.sql
db2 "load from .\setup\data\topic\mydiagnoses.txt of del modified by
coldel| identitymissing insert into DiseaseDiagnosisCode"
db2 connect reset
```

Observations or lab codes

The predefined data for observation codes are contained in the following file in the <HCN_Admin_Server_Install_Root>\database\setup\data\topic directory:

loinc_codes.txt

The names of the files and database tables refer to these as *lab codes*. However, they cover a larger part of the clinical domain than just the laboratory, including the entire range of clinical observations.

The format of these files is that each line contains an observation code, a name, a property, a system, and a method type, each separated by a vertical bar (or pipe, “|”) delimiter. The database table itself contains a generated ID column plus these five fields. The generated ID column is accounted for by using the modified by identitymissing clause on the DB2 **load** command.

To replace the pre-installed observation table with a different set of observations codes, first create or acquire a file that contains the observation codes in this format. Coding systems other than LOINC might not have all of these fields (for example, system or method type). You can use blank values for all values except the name, and you can omit trailing delimiters. For this example, we assume the file is:

```
<HCN_Admin_Server_Install_Root>\database\setup\data\topic\
myobservations.txt
```

Open a DB2 command window and issue the commands that are shown in Example A-7.

Example: A-7 Replacing the pre-installed observation table

```
db2 connect to HCN_DB
db2 drop table LabTestCode
cd <HCN_Install_Root>\Administrative Server\database
db2 -td; -f.\db\topic\user\lab_test_code.sql
db2 "load from .\setup\data\topic\myobservations.txt of del modified by
coldel| identitymissing insert into LabTestCode"
db2 connect reset
```

Customizing HCN privacy rules

HCN transmits clinical data about individual patients. Therefore, it is necessary that the HCN meet the privacy and security requirements for data confidentiality, integrity, authentication, authorization, and non-repudiation. The HCN system is predefined with three privacy levels to manage patient identification. Each privacy level defines the fields in the clinical messages that must be removed or modified before these messages can be exchanged in the network.

The HCN system supports the capability to modify the de-identification routines and to create additional de-identification levels for HL7 messages.

Modifying existing privacy levels

The definitions and actions for the three predefined de-identification levels are implemented using Python in Chameleon message definition files. Table A-1 lists the definition files.

Table A-1 Message definition file list

De-identification level	Location of the message definition file
FullyIdentified	<PublisherGateway_Root>\vmd\FullyIdentified.vmd
HIPAAALimitedDataSet	<PublisherGateway_Root>\vmd\HIPAAALimitedDataSet.vmd
HIPAAAFullyDeidentified	<PublisherGateway_Root>\vmd\HIPAAAFullyDeidentified.vmd

Note: The <PublisherGateway_Root> directory is the installation directory for the publisher gateway. In our scenario, <PublisherGateway_Root> is C:\HCN\Gateway\Publisher Gateway.

To customize the rule for an existing de-identification level, follow these steps:

1. Open the FullyIdentified.vmd file with iNTERFACEWARE Chameleon tool.
2. All supported HL7 messages are listed in the Messages folder on the left-hand pane. Expand the object tree by clicking each plus symbol (+), as shown in Figure A-25 on page 213.

Note: Examine the Segment Grammar object in the expanded list. The segment grammar definition that is provided by Chameleon is the representation of the definition of the message type by HL7.

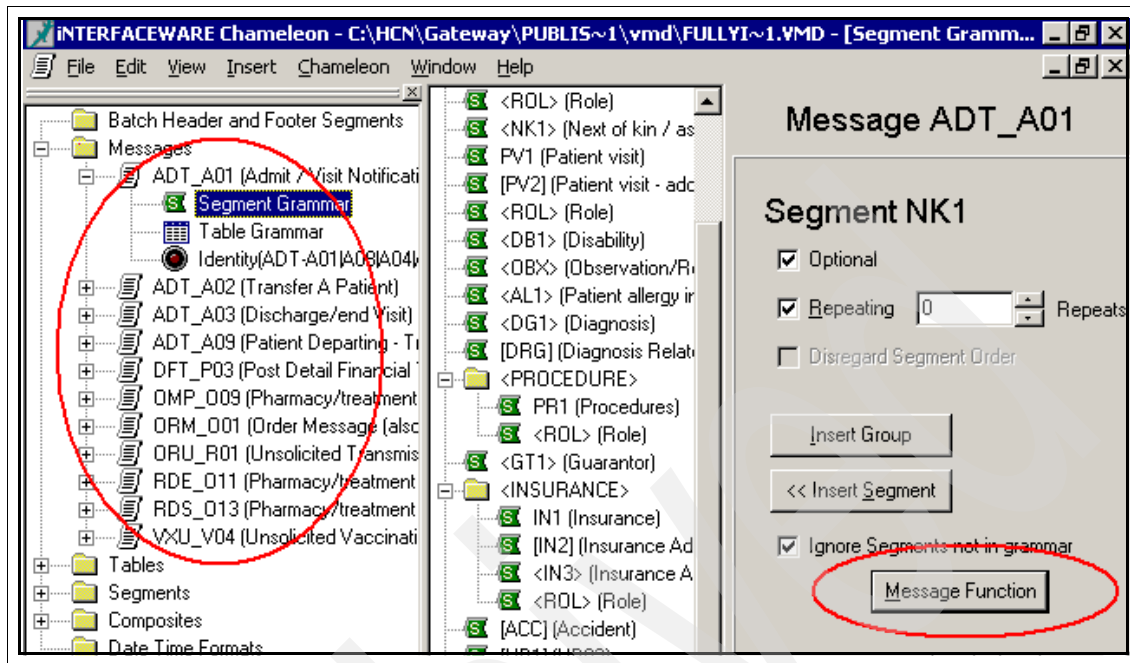


Figure A-25 Browsing Pass-through mapping project

3. Click **Message Function** to view the Chameleon message pass-through mapping function written in Python script language.

Note: Message function generally creates a *segment iterator* object. The segment iterator enables the Python code to access the messages being transformed, segment by segment. The iterator gives the code the ability to get and change values in each segment and then generate the modified version. Example A-8 shows the sample code for ADT_A01 message.

Example: A-8 Sample Python code for privacy control

```
# the module function deidentifyMessage is contained in the module
# FullyIdentified.py which
# is imported via the inbound equation

# the AGPI and the Assigning Authority are passed to the VMD from the calling
# program
lid = AGPI
laa = AUTH

# Get an iterator that points to the first segment
iterator = environment.input_segment_iterator()
```

```
#no transformation for first (MSH) segment
output = iterator.output()

while (iterator.move_one()):
    # call the deidentification function that is contained in the module
    LimitedDataSet.py
    deidentifiedSegment = deidentifyMessage(iterator, lid, laa)
    output = output + deidentifiedSegment

value = output
```

4. In the first and second highlighted lines of the python code, we assign the Anonymous token (an Anonymous Global Patient Identifier, or AGPI) and the Assigning Authority to Python temporary variables. The anonymous token and assigning authority are retrieved from AGPI server, then passed from the Gateway_to_Broker_Deidentification collaboration object to the Python message function through the Chameleon API as global variables.
5. In the third highlighted line of the python code, we get a segment iterator object and then pass it to the Python function named `deidentifyMessage()`. The `deidentifyMessage()` function is contained in the module `FullyIdentified.py`, which is imported via the inbound equation. You can find the inbound equation by selecting **Chameleon** → **Inbound Equation**. Example A-9 shows the equation sample.

Example: A-9 Chameleon inbound equation

```
from FullyIdentified import *
```

Note: The Python script file `FullyIdentified.py` is located in the `<PublisherGateway_Root>\scripts` directory. Example A-11 on page 217 shows the sample code for the `deidentifyMessage()` function.

Note that Python scripts do not use a begin block and end block character, because curly braces (`{` and `}`) are used in C or Java. Instead, begin block and end block are controlled by indentation. Therefore, when editing Python scripts, pay close attention to whether lines are indented using a tab character or spaces, and follow a consistent practice when indenting lines.

6. In the version of the `FullyIdentified` de-identification level that HCN provides, the script replaces the value in PID.3.1 (the first sub-field of the Patient Identifier List field in the PID segment of ADT_A01 message) with the anonymous token and replaces the value in PID.3.4 with the Assigning Authority.

7. To understand how the Chameleon pass-through mapping works, we test the pass-through mapping using the Test Mapping function of Chameleon, which can be accessed through the Chameleon menu. However, the Test Mapping function does not support the global variable mechanism that HCN uses to pass the AGPI and Assigning Authority values. So, we modify the script temporarily to use hard-coded values. Modify the first portion of the message function for message ADT_A01, as shown in Example A-10.

Example: A-10 Modified message function

```
# the AGPI and the Assigning Authority are passed to the VMD from the calling
program
#lid = AGPI
lid = 'AGPI-0000000001'
#laa = AUTH
laa = 'HCN Gateway'
```

8. Click **Chameleon** → **Test Mapping** to open the Test Mapping window.
9. Paste a test HL7 message of type ADT_A01 into the upper input box and select **Pass-through Mapping**.
10. Click **Transform** and select the transformed HL7 messages, as shown in Figure A-26 on page 216.

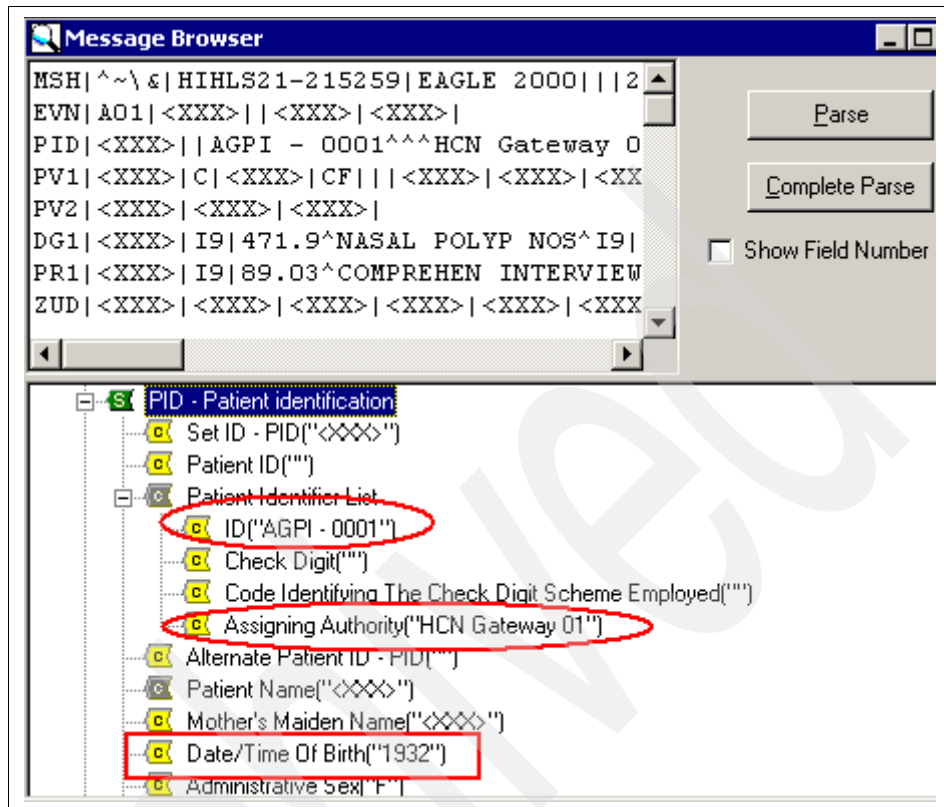


Figure A-27 Testing result

12. To modify the rule for FullyIdentified de-identification level so that it clears the date of birth in the seventh field in the PID segment, modify the Python script FullyIdentified.py and add the statement in the deidentifyMessage() function, as shown in Example A-11.

13. Save the script file.

Example: A-11 Customize the script used for privacy control

```
def deidentifyMessage(iterator, localID, assigningAuthority):

    if iterator.segment_id() == 'PID':
        iterator.field(3).subfield(0).value = localID
        iterator.field(3).subfield(3).value = assigningAuthority

        iterator.field(7).clear()

    return iterator.output()
```

```
else:  
    return iterator.output()
```

14. Close Chameleon and re-open the FullyIdentified.vmd project to refresh the Python environment and to pick up the changes to the script.

15. Repeat these steps to verify that the new rule has been applied.

The result shows the date of birth field is cleared, as shown in Figure A-28 on page 218.

Remember to remove the temporary changes you made to the script in the VMD file for testing purposes.

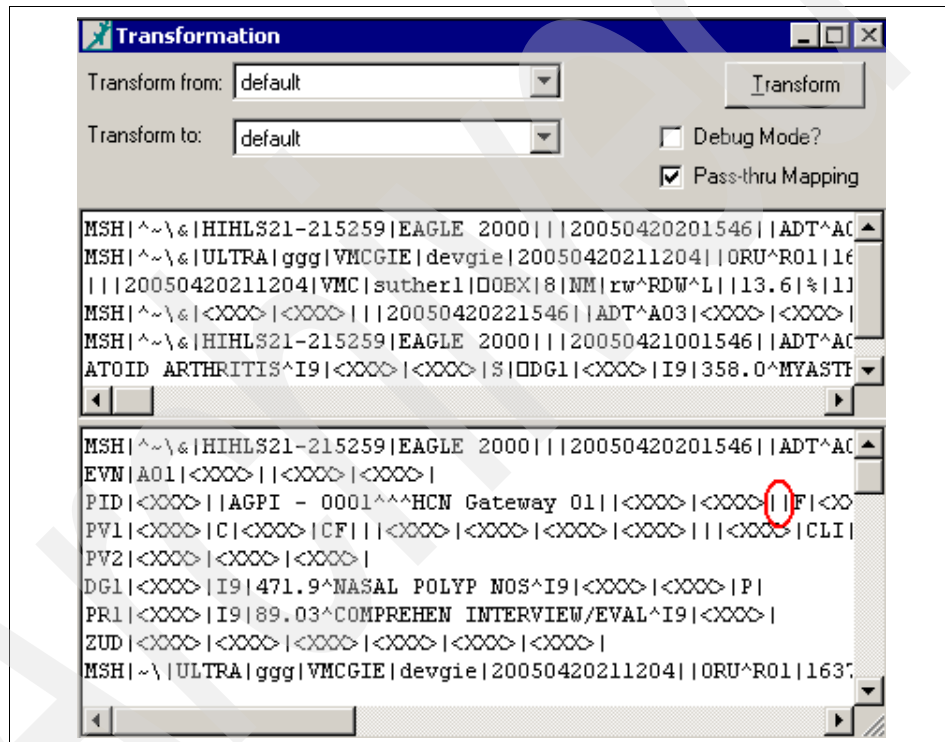


Figure A-28 View testing result

After following these steps, you can see how HCN uses mapping tools and content filtering capabilities that are provided by the INTERFACWARE Chameleon HL7 toolkit to achieve the flexible implementation that is required for privacy.

Creating and deleting privacy levels

To modify the implementation of the existing privacy levels, no further steps are required. When you restart the HCN Publisher Gateway, the Gateway uses the modified Chameleon VMD files and Python scripts.

HCN also allows you to create and to delete privacy levels. To create the de-identification implementation for privacy levels, you can follow the steps to create a new VMD file and associated external python scripts. For ease of administration, the name of the VMD file should be the same as the name of the privacy level.

For the Gateway to be aware of the new privacy level implementation, follow these steps:

1. Place your Chameleon message definition file (.VMD) in the directory that is defined in the `DEIDENTIFICATION_FILE_DIRECTORY` property of the `Gateway_to_Broker_Deidentification` collaboration. The default path in HCN is `<PublisherGateway_Root>\vmd` directory.
2. Place your Python function modules, which have the extension .py, in the directory that is defined in the environment variable `CHM_PYTHON_LIB_PATH`. The default path in HCN is `<PublisherGateway_Root>\scripts` directory.

Note: You must use the DOS 8.3 short name format (without spaces) in the environment variable.

Note: The embedded Python engine in Chameleon looks for python scripts first in the same directory as the `CHM_LIB3.dll` file. The next directory is the subdirectory `lib`. Additionally, you can specify other locations with the environmental variable `CHM_PYTHON_LIB_PATH`. The HCN Gateway installation program sets the `CHM_PYTHON_LIB_PATH` environmental variable for you.

3. Update the `DEIDENTIFICATION_VMD_FILES` property of the `Gateway_to_Broker_Deidentification` collaboration in the WebSphere Business Integration Workbench System Manager. Add (or remove) a key/value pair for the de-identification level name and VMD file that you have added (or deleted).

For example, a key/value pair of the following:

```
HIPAALimitedDataSet;HIPAALimitedDataSet.vmd
```

Means that for the level `HIPAALimitedDataSet`, it uses the definition file `HIPAALimitedDataSet.vmd` to de-identify the messages (Figure A-29 on page 220).

4. Update the DEIDENTIFICATION_LEVELS property of the Portal_to_Gateway_HCN_TopicSync collaboration to include (or remove) the added (or deleted) privacy levels.

Property name	Value
1 DEIDENTIFICATION_FILE_DI...	C:\HCN\Gateway\Publisher Gateway\vmd\
2 XML_MESSAGE_TYPES	CDA;MAGE;BSML;ODM;HAPMAP
3 DEIDENTIFICATION_VMD_FILES	HIPAAALimitedDataSet;HIPAAALimitedDataSet.vmd;HIPAAFullyDeidentified;HIPAAFullyDei...
4 DEIDENT_LIMITED_DATA_SE...	FALSE
5 ANONYMIZATION_CONFIG_X...	C:\HCN\Gateway\Publisher Gateway\Config\anonymization-config.xml
6 ANONYMIZATION_CONFIG_D...	C:\HCN\Gateway\Publisher Gateway\Config\anonymization-config.dtd
7 EnableInstanceReuse	true
8 LOGGING_DATASOURCE	/log.properties
9 ANONYMIZATION_CONFIG_D...	anonymization 1.0

Figure A-29 Applying new privacy code to collaboration

Before users can create topics that use the privacy levels that you have defined, you must modify the database on the HCN Administration Server to reference the privacy levels. Then, an HCN Administrator must modify the definitions of the organizations and gateways to indicate their ability to support the privacy level.

If you intend to remove any privacy levels from your HCN system, before you modify the database on the HCN Administration server, you must delete all topics that refer to the privacy levels that you intend to delete and remove the privacy level association from each gateway and organization that supports it. This can be done by an HCN Administrative user, except that topics must be deleted by the same user that created them. See Chapter 4, “HCN entities and functional components” on page 97 for detailed instructions about how to manage organizations and gateways.

To add or delete privacy levels on the HCN Administration server, you must update the database directly.

To delete a privacy level (after removing references to it as described), issue the following commands in a DB2 command window.

```
db2 connect to HCN_DB
db2 delete from PrivacyLevels where PrivacyIdentifier='name'
db2 connect reset
```

In this command, *name* refers to the name of the privacy level as used by the gateway.

To insert a privacy level, you must provide three values on an SQL command:

1. A short name for the privacy level for display purposes(maximum 50 characters)
2. A longer description for the privacy level (maximum 512 characters)
3. The exact name of the privacy level as used on the gateway (maximum 50 characters)

To insert the privacy level into the database, issue the following commands in a DB2 command window (replacing the italicized parameters with the three values listed previously):

```
db2 connect to HCN_DB
db2 insert into PrivacyLevels (PrivacyLevel,Description,Identifier)
VALUES('shortName','description','exactName')
db2 connect reset
```

You must restart the Administration Server to pick up the changed database values.

De-identifying XML messages

When using HCN as part of the IBM Clinical Genomics version 2 solution, you might need to de-identify XML documents using the concept of de-identifying privacy levels . The process of de-identifying XML documents does not use Chameleon (as for HL7 messages) but instead uses a configurable XML transformation framework that uses XSLT and XPATH.

This book does not provide detailed examples of using HCN with Clinical Genomics version 2. We provide a description of the steps that are required to configure de-identification of XML documents. To modify the implementation of an existing privacy level for XML documents:

1. On the publisher gateway, open the following file in the <HCN_Install_Root>\Config directory:
anonymization-config.xml
2. Find the XML element <de-identification-domain> with a type attribute of the concatenation of the document type and the privacy level name, all converted to lowercase.
3. Edit the XPATH location of the information to be de-identified (node-selector attribute) or the action to be performed (action-name attribute) for each child <task> element in the file, or add new <task> elements if additional items are to be de-identified.
4. Restart the Publisher Gateway to force the gateway to re-load the XML de-identification configuration file.

To create or remove privacy levels for XML documents:

1. On the publisher gateway, open the following file in the <HCN_Install_Root>\Config directory:
anonymization-config.xml
2. Create or remove the <de-identification-domain> sections as desired.
3. Follow the instructions in “Creating and deleting privacy levels” on page 219 to update the collaboration properties and HCN Administration Server with the new privacy level names.

Consolidating HL7 messaging variation

The HL7 standard is intended to standardize data interchanges, not the underlying application systems. Thus, there will be a wide variety in the manner in which the standard is applied in different institutions.

HCN Gateway has the capability to transform HL7 messages that it receives to the correct nonstandard local HL7 usage or convert older HL7 messages to newer versions. This feature is similar to replacing local codes with standard codes, as described in “Mapping local clinical codes” on page 203.

The Pass-through Mapping function of Chameleon is what you use to implement the transformation function. To transform incoming message format to our HCN canonical HL7 2.4 message format, the Hospital_to_Gateway_Entry::HCN_Entry collaboration invokes the dynamic engine to get the message format for parsing and the Python scripts for performing the transformation from message definition files (VMD). The HL7 message parsing engine first obtains the HL7 version field from the header, then it invokes the appropriate pass-through mapping functions for the HL7 version.

Because the Hospital_to_Gateway_Entry::HCN_Entry collaboration leaves only one property to define the external message definition file which is used for message transformation, all transformations must take place in the same VMD file. So, for example, if you are using the transformation code for local code mapping, as described in “Mapping local clinical codes” on page 203, you must merge any additional transformation required into the same VMD file. Be sure to turn on the translation function by updating the TRANSLATION property to TRUE and making the TRANSLATION_VMD property point to the new message definition file that you create.

As an example, consider the following sample message which contain a HL7 V2.1 messages for observation results:

```
MSH|^~\&|<XXX>||<XXX>|<XXX>|20040422234705||ORM|<XXX>|<XXX>|2.1
PID|||219735||<XXX>||1918|F|||||||<XXX>
PV1|||<XXX>
ORC|RE|||||36738^QUANTITY NOT SUFFICIENT NOTIF+|||||||<XXX>
OBR|||H56788HCOAG 044M^1|59723^MED^COAG PROFILE|||20040422231000|
OBX|1|ST|5902-2^LOINC^PT|0|ORD|sec
OBX|2|ST|6301-6^LOINC^INR|0|""
OBX|3|ST|14979-9^LOINC^APTT|0|ORD|sec
OBX|4|ST|3255-7^LOINC^FIBRINOGEN|0|""|mg/dl
OBX|5|ST|3243-3^LOINC^THROMBIN TIME|0|""|sec
```

In addition, this message appears to have nonstandard usage of the Observation ID field, because the subfields are in the wrong order. (Certain fields not relevant to this example are shown as <XXX> or truncated.)

Example A-12 shows the message transformation script that converts the message to HL7 v2.4 with the correct the nonstandard usage.

Example: A-12 Sample code for consolidating various HL7 message

```
# Get an iterator that points to the first segment
iterator = environment.input_segment_iterator()

# The iterator starts out on the first segment - i.e the MSH segment.
# This is a ORU message with no event type... Change it to an ORU^R01
iterator.field(9).value = "ORU^R01"

# Change the version to 2.4
iterator.field(12).value = "2.4"
output = iterator.output()

# move to the PID segment and include it unchanged
if iterator.move_next('PID'):
    output = output + iterator.output()

# move to the PV1 segment and include it unchanged
if iterator.move_next('PV1'):
    output = output + iterator.output()

# move to the ORC segment and include it unchanged
if iterator.move_next('ORC'):
    output = output + iterator.output()

# move to the OBR segment and include it unchanged
if iterator.move_next('OBR'):
    output = output + iterator.output()
```

```
# move to the OBX segment and correct the order of the subfield of field 3
while iterator.move_next('OBX'):
    f0 = iterator.field(3).subfield(0).value
    iterator.field(3).subfield(0).value = iterator.field(3).subfield(1).value
    iterator.field(3).subfield(1).value = iterator.field(3).subfield(2).value
    iterator.field(3).subfield(2).value = f0

# add a OBX.11 value of 'F' if the field isn't present
if iterator.field(11).is_null():
    iterator.field(11).value = 'F'

output = output + iterator.output()

value = output
```

Health Level 7 overview

This appendix provides a high level overview of the Health Level 7 (HL7) protocol. The goal is not to teach you all there is to know about HL7. Instead, this appendix introduces a few key points to enable you to understand HL7 messaging. We assume that if you are reading this appendix, that you are interested in learning what HL7 is, how it is structured, and how HL7 messages are parsed in general.

This appendix includes the following sections:

- ▶ Introduction to Health Level 7
- ▶ HL7 message structure
- ▶ Structural presentation of HL7 messages
- ▶ Types of HL7 messages

Introduction to Health Level 7

HL7 stands for *Health Level 7*, where *Level 7* refers to the seventh layer of the International Organization for Standardization (ISO), Open Systems Interconnection (OSI). In OSI parlance, this layer is referred to as the *application layer*. Figure B-1 illustrates the OSI model.

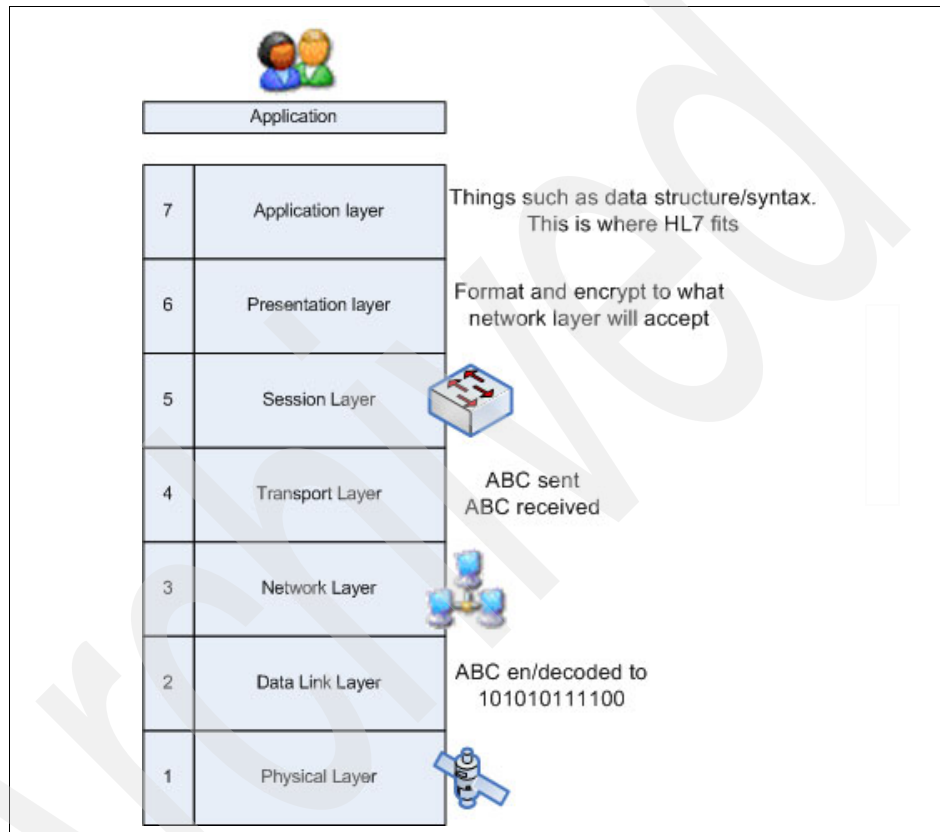


Figure B-1 OSI stack.

HL7 was proposed as a healthcare messaging standard in the late 1980's to address the growing issue of system interoperability within the healthcare space. (Version 1 of the standard was published in 1987 and version 2.4 was published in 2000.) HL7 is both the name of the standards development organization and the name of the set of protocols that the organization publishes. It is a worldwide standard with affiliate chapters in several countries. There are HL7 affiliates throughout the world, including the Americas, Europe, and Oceania, that contribute their expertise to the overall standards development effort. HL7 is

American National Standards Institute (ANSI) accredited and an approved Standards Developing Organization (SDO).

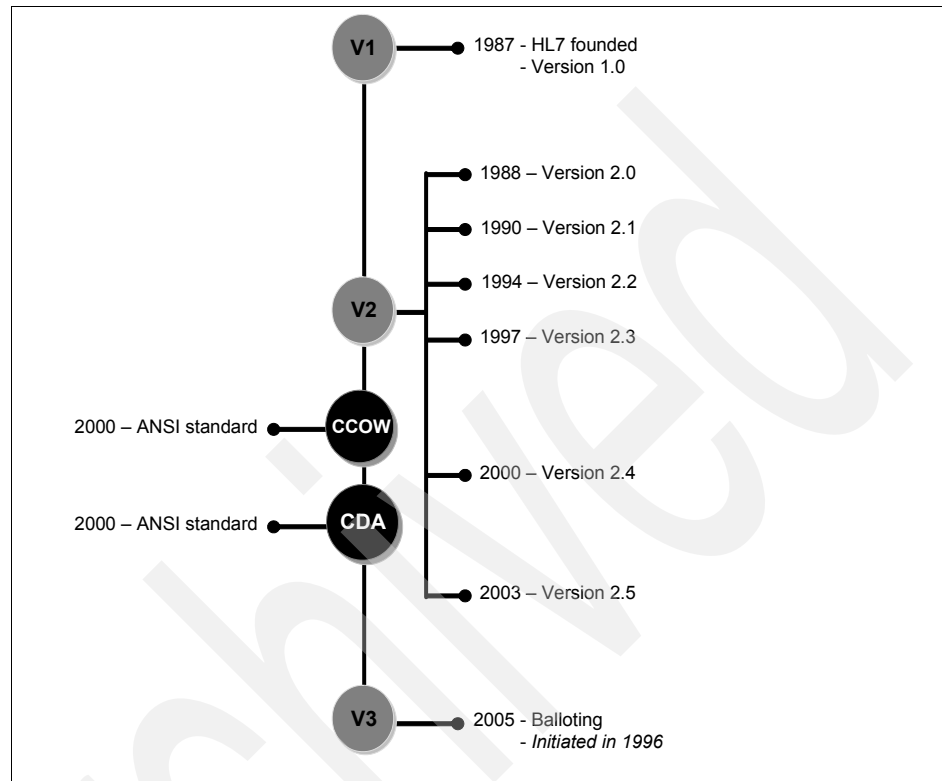


Figure B-2 HL7 standard timeline

Note: For more detailed information about how to get HL7 in your local area consult the following or your local standards body:

<http://www.HL7.org>

Selecting **International Affiliates** provides a list of International HL7 affiliates with contact information for each.

HL7 was designed around the *lowest common denominator* approach. In other words, anyone with a text editor should be able to create HL7 messages by following a few simple rules. There are numerous means for transporting HL7 messages between systems, including simple file transfer (at the application layer of OSI) and other OSI transport mechanisms, such as TCP/IP.

Although HL7 messages can be transported through just about any means that can connect two systems, file transfer and lower-level OSI transport protocols are the most used transport mechanisms for HL7 messaging.

Note: Transport mechanisms that make use of the OSI lower level transport protocols such as TCP/IP are referred to as Lower Layer Protocols (LLP). Though lower-layer protocols are not part of the HL7 standard specification, you can find information about them in the HL7 Implementation Guide.

HL7 message structure

A given HL7 message consists of one or more segments. Each segment starts with a three character identifier and ends with a segment separator. Segments are defined to be either required or optional and can be repeated. A segment consist of logically grouped variable length data fields that are separated by data field delimiters. The hierarchical structure of a message is as follows:

1. One or more segments, which are repeatable.
2. Data fields (also referred to simply as *fields* within this document), which are also repeatable.
3. Components that are contained within a data field.
4. Sub-components that contained within a component.

The first segment of an HL7 Message must be the Message Header (MSH) segment. The message must be terminated by a sequence of message terminator characters. It should be noted that the termination characters need not be a visible character. For example, an HL7 message could be terminated with a [carriage return] [line feed] character sequence (that is, ASCII characters 0x'0D' + 0x'0A') or a sequence of characters such as this-message-ends-here. Most HL7 implementations use the [carriage return] [line feed] character sequence as the message terminator.

Figure B-3 illustrates the hierarchical relationship of the structure of HL7 messages.

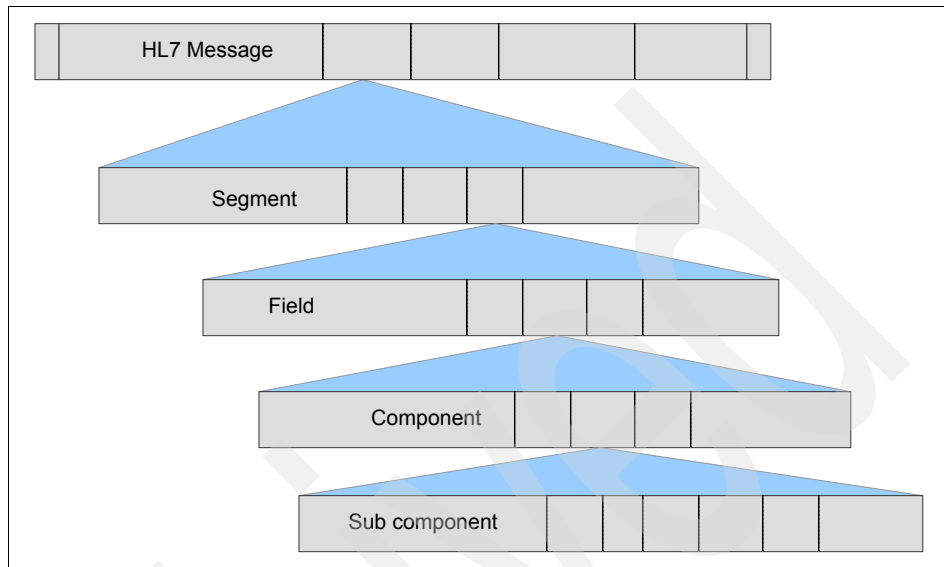


Figure B-3 HL7 message structure artifacts

Components and sub-components are two data types in the definition tree that control the content type of fields. For example, in one segment you can have a field defined and called *PatientID* and assigned integer data type. In another segment (or even the same segment), the same data could be present in a field called *MedicalReferenceNumber* but this time, it is assigned string data type. In addition to its basic function, a field's data type also controls whether the field contains components.

Note: For the purposes of this appendix, we do not delve deeper into data type definitions and their influence on HL7 messages. It is sufficient for us to consider every field to be simply a long string of characters.

HL7 standard also supports the following capabilities:

► Define content length

For example, the patient name field in the patient identification segment (PID) has room for 48 characters.

► Repetition

Within the HL7 V2.X standard is the ability to assign repetitive capabilities to message artifacts. For instance, some segments, such as the observation

(OBX) segment can be present in an HL7 messages a number of times. It is also possible to repeat fields, component, and sub-component structures within HL7 messages.

- Denote field type

Some of the complexities of HL7 2.x include the ability for one field to denote the data type of a following field. For instance, in the OBX segment, the second field is used to denote the data type of the fifth field.

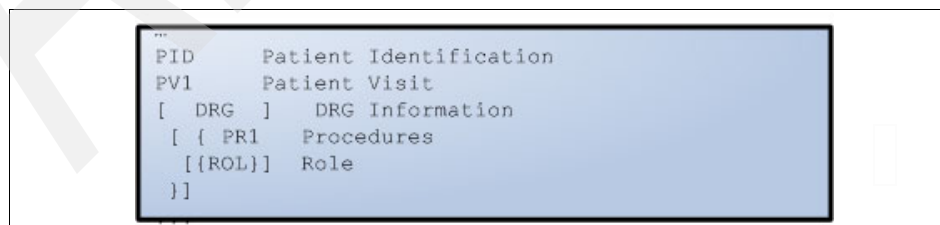
Structural presentation of HL7 messages

HL7 developed during a time when the present standards for complex structural presentation (such as those used in XML schemas today) were not available. It is a credit to the people that created the standard that they were able to present a complex field of endeavour — structural presentation of HL7 message constructs — in a simple graphical form.

The format they use to present messages focusses on the segment level construction of HL7. Segments can be optional, can repeat, and are sometimes mandatory, depending upon the information they are conveying. In order to present this, three basic presentations were developed.

- For optional message segments, HL7 presents the segment contained within braces (curly brackets).
- For repeating segments, HL7 presents the segment enclosed in square brackets.
- Mandatory, non-repeating segments are presented with no surrounding characters.

Finally, HL7 presentation provides the facility to denote segment groupings (that is, segments that have a relationship to some parent segment). Take, the partial message structure definition for a certain type of HL7 message that is shown in Figure B-4.



```
...
PID      Patient Identification
PV1      Patient Visit
[ DRG ]  DRG Information
[ { PR1  Procedures
  [{ROL}] Role
  }]
...
```

Figure B-4 HL7 identification information example

This structural presentation is conveying the following about this message, the patient identification (PID) and patient visit (PV1) segments are mandatory while the diagnostic or diagnosis related group segment (DRG) is optional. In addition to these segments, should the DRG segment be included, then the message has the option of containing multiple procedure segments (PR1). Each procedure segment, in turn, has the option to contain multiple role segments (ROL).

This might sound confusing, but it is fairly simple. When you see such a message, in which this construction is present, all you are presented with is one segment after another, displayed as a stream of characters. What the structural presentation conveys is that there are certain contextual relationships between the segments at which you are looking.



Figure B-5 Segments strung together

HL7 also allows for user definable segments, called *z-segments*, which means that any additional (beyond the scope of the HL7 standard) information can be transmitted in a z-segment (whose three-letter segment identifier begins with the letter *z*), so long as the concerned parties agree and maintain the structural integrity.

Types of HL7 messages

HL7 messages carry the concept of event types within their structure. These event types allow us to process the messages appropriately. Event types can also be used to initiate complex behavior in the processing system. For example, in our scenario, there is no specific pandemic alert message construct. However, a HL7 observation reporting event message is able to convey enough information for HCN to initiate a public health alert.

HL7 messages fall into several broad categories:

- ▶ Admission, Discharge, and Transfer (ADT)
- ▶ Finance
- ▶ Master Files
- ▶ Order Entry
- ▶ Observation Reporting
- ▶ Query
- ▶ Acknowledgement (/negative acknowledgement)

Admission, Discharge and Transfer (ADT-A01)

```
MSH      Message Header
EVN      Event Type
PID      Patient Identification
[PD1]    Additional Demographics
[ { NK1 } ] Next of Kin / Associated Parties
PV1      Patient Visit
[ PV2 ]  Patient Visit - Additional Info.
[ { DB1 } ] Disability Information
[ { OBX } ] Observation/Result
[ { AL1 } ] Allergy Information
[ { DG1 } ] Diagnosis Information
[ DRG ]  DRG Information
[ { PR1 } Procedures
[ { ROL } ] Role
}]
[ { GT1 } ] Guarantor Information
[
  { IN1 } Insurance Information
  [ IN2 ] Insurance Information - Addit. Info.
  [ IN3 ] Insurance Information - Cert.
]
]
[ ACC ]  Accident Information
[ UB1 ]  Universal Bill Information
[ UB2 ]  Universal Bill 92 Information
```

Admission, Discharge and Transfer (ADT-A32)

```
ADT-A32
MSH      Message Header
EVN      Event Type
PID      Patient Identification
[PD1]    Additional Demographics
PV1      Patient Visit
[ PV2 ]  Patient Visit - Additional Info.
[ { DB1 } ] Disability Information
[ { OBX } ] Observation/Result
```

Admission, Discharge and Transfer (ADT-ACK/NAK)

```
MSH      Message Header
MSA      Message Acknowledgment
[ ERR ]  Error
```

Figure B-6 HL7 message types

HL7 supports the use of codes such as LOINC and SNOMED and well as ICD within its message structures.

HCN supports HL7 version 2.4 messages from the ADT, Order Entry, and Observation Reporting domains. Since HL7 version 2, messages are backwards compatible, messages of version 2.1, 2.2, 2.3, and 2.3.1 are also supported by HCN. In addition, the HCN Publisher Gateway combined with the Medical Information Repository feature of the IBM Clinical Genomics version 2 solution can be used to transfer HL7 Clinical Document Architecture (HL7-CDA) Level 2 documents to a clinical data repository.

HCN is able to interact with HL7 messages on both the full message and individual artifact level, hence HCN is aware of the information represented within the message. HCN is able to use such information for topic evaluation purposes.

Note: HL7 messages are neither private nor secure. Privacy and security are functions of the infrastructure through which the messages travel. Refer to Chapter 6, “Privacy and security” on page 165 for a description of privacy and security in HCN.

The MSH segment

Every HL7 version 2 message contains an MSH (message header) segment. The MSH segment identifies the message type, contains a message time stamp, unique sequence number (unique from the point-of-view of the sending application), and other metadata about the message, such as the version ID and language.

Importantly, the first two fields of the MSH segment contain the parsing characters that are necessary to correctly parse the message. These characters are the field separator, component separator, sub-component separator, repetition separator, and escape character.

The HL7 specification allows each of these parse characters to be defined within the message itself. Parsing applications must read the parse characters and parse the message accordingly. Fortunately for humans attempting to read the message in a text or log file, the HL7 suggested values are widely used.

Table B-1 lists the HL7 suggested parse characters.

Table B-1 HL7 suggested parse characters

Parse Character	Suggested Value
Field Separator	
Component Separator	^
Sub-component Separator	&
Repetition Separator	~
Escape Character	\

The separator between segments is defined by HL7 to be the carriage return (0x0D) character, and cannot be modified by an implementation. All HL7 messages must end with the line feed (0x0A) character following the carriage return which ends the final segment in the message.

Due to the non-assured delivery of the LLP (TCP/IP is commonly used), HL7 messages use a specific message to acknowledge positive receipt of the message and negative receipt of the message. The acknowledgment message contains a message header (MSH segment), an acknowledgement (MSA segment), and optionally an error segment (ERR). For all HL7 messages, segment order must be compliant with the order that is defined in the HL7 specification.

You can find the detailed HL7 message specification at:

<http://www.hl7.org>

Approved HL7 specifications are available for purchase. HL7 members can download the specifications.

Performance tuning

This appendix provides guidelines for tuning your HCN solution to improve performance. It identifies the components where performance tuning is appropriate and the steps that you need to take.

Of the four components of the HCN solution, the Gateway and the Message Flow Server are likely to be the points that are sensitive to performance issues. You can tune the Administration Server and the AGPI server using standard practices for tuning applications in WebSphere Application Server.

This appendix includes the following sections:

- ▶ Publisher gateway performance
- ▶ HCN subscriber gateway performance
- ▶ WebSphere Business Integration server performance
- ▶ HCN Message Flow server performance
- ▶ Database performance

Publisher gateway performance

You can achieve significant performance improvement of the HCN by tuning the publisher gateways. This section identifies the various performance issues and then describes how you should address these issues.

Polling

The first performance issue is the handling of incoming messages from the HL7 applications. These points do not apply to incoming XML messages, because XML messages are not evaluated by the gateway but are merely passed through based on the existence of a topic which names that XML document type. HL7 messages take a two-step path through gateway, as shown in Figure C-1.

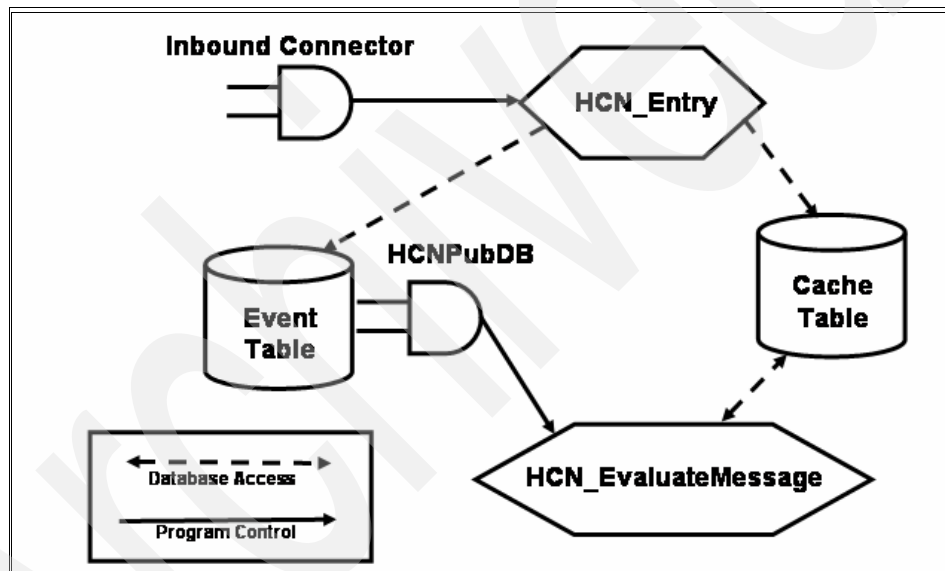


Figure C-1 HL7 Message evaluation flow

The inbound connector (either the HCNHL7 connector, HCNEventFile connector, or HCNEventQueue connector) receives the HL7 message from the incoming application (over a socket connection, file, or MQ queue, respectively). The inbound connector then passes the message to the HCN_Event collaboration, which determines the patient ID, assigns an anonymous ID, and writes the message to the database cache. It also writes a record in an event table to trigger the next step in the message flow. However, only one event record is written for each anonymous patient ID, allowing multiple messages for the same patient to be processed only once.

The HCNPubDB connector reads the event records from the event table and triggers the HCN_EvaluateMessage collaboration, which retrieves the set of messages for a patient from the database cache and evaluates them against the topics being published by the gateway. The HCN_EvaluateMessage collaboration sends messages to the HCN Message Flow Server in publications based on the results of this evaluation.

To optimize the performance of the message evaluation flow, the HCNPubDB connector should be configured to allow multiple messages for the same patient to be processed in one evaluation, by setting the poll frequency property of the connector. Consider the arrival rate of incoming HL7 messages, and the tendency of the sending applications to send multiple messages for the same patient in batches. You should also consider the needs of the HCN subscribers to receive publications for their subscribed topics in real-time, or near real-time.

For example, if nurses in a hospital ward tend to enter all of the medication orders for a given floor into the pharmacy order system at the end of rounds, and the process of entering the orders takes 10 minutes, then a poll frequency of at least 20 minutes would capture all of the pharmacy orders for the same patient in a single polling interval. The poll frequency of the connector is specified in milliseconds, so to configure 20 minutes, set the poll frequency to 1200000. See Figure C-2 on page 238.

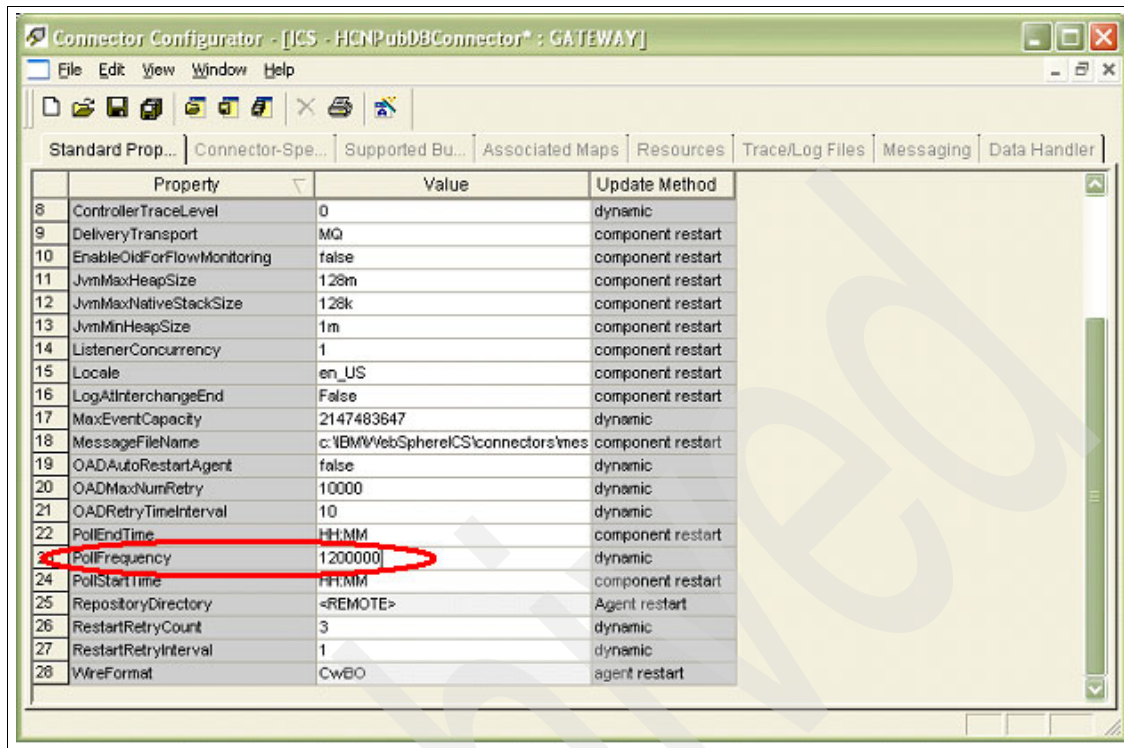


Figure C-2 Connector Configuration showing Poll Frequency

When setting the HCNPubDB poll frequency to values of 10 minutes or higher, you might also want to increase the `PollQuantity` property of the connector (located on the Connector-Specific properties tab of the Connector Configurator) to allow more messages to be processed each polling interval. You can use the statistics capability of the System Manager to watch the runtime performance of the of the WebSphere Business Integration Server to determine whether it is processing all messages during each polling interval. The number and complexity of the topics being published by the gateway will have a significant effect on the performance of the `HCN_EvaluateMessage` collaboration.

The second factor which impacts the performance of the HL7 message evaluation flow is the number of threads being utilized by the WebSphere Business Integration Server to perform the evaluation. As shipped, the HCN collaborations use only a single thread. You can improve performance by allocating multiple threads to the collaborations, especially on systems with multiple CPUs.

The optimum number of threads to use can be determined by watching the WebSphere Business Integration Server performance using the statistics view of the System Manager. A good starting value would be five threads. It is unlikely that increasing the number of threads beyond 10 would result in additional performance increases.

To change the number of threads, modify the collaboration properties for each of the following collaborations to set the Maximum number of concurrent events property (see Figure C-3 on page 240):

- ▶ Hospital_To_Gateway_Entry
- ▶ Gateway_to_Broker_Evaluate
- ▶ Gateway_to_Broker_Deidentification
- ▶ Gateway_to_Broker_CDAConstruktor
- ▶ Hospital_to_Gateway_AGPI

Properties

Collaboration General Properties | Properties

Create from template:

Effective transaction level: Minimum transaction level:

System Trace Level: Collaboration trace level:

Email notification address:

☐ Pause when critical error occur Maximum number of concurrent events:
☐ Persist Service Call in Transit State Recovery Mode:
☒ Implicit Database Transaction Max Event Capacity:
☒ Blocking Type

OK Cancel

Figure C-3 Collaboration threading properties.

You should set the same value for Maximum number of concurrent events in all five collaboration objects, and you must also set the ListenerConcurrency and ConcurrentEventTriggeredFlows properties of the HCNPubDB connector to the same value.

Gateway connector performance

There are performance considerations for both the HCNHL7 Connector and the HCNEventFile Connector. For the HL7 connector, flow control is implemented to prevent the queue between the HCNHL7Connector and the WebSphere Business Integration Server (AP/HCNHL7Connector/WebSphereServer) from being overrun

with messages. This flow control is configured through two properties of the HCNHL7 connector:

- ▶ `MaxMessageQueueDepth` (default 500)
- ▶ `HL7ResponseDelayWhenCongested` (default 500 ms)

The flow control algorithm is triggered when the number of messages on the in-memory buffer used by the connector exceeds `MaxMessageQueueDepth`. This usually would occur only if the MQ queue `AP/HCNHL7Connector/WebSphereServer` has exceeded its maximum depth and the connector controller has stopped polling. When flow control is triggered, the connector delays each HL7 acknowledgement by the amount of time specified in `HL7ResponseDelayWhenCongested`. This allows the sender to continue sending messages, but at a much slower rate. Normal responses (no delay) resume when the number of messages in the in-memory buffer falls below `MaxMessageQueueDepth`.

To optimize performance, configure the maximum depth of the MQ queue large enough to handle bursts in HL7 traffic and avoid triggering the flow control algorithm. Of course, following the recommendations of the preceding section to improve the performance of the evaluation collaboration helps ensure that messages are removed from the queue and processed promptly.

When using the `HCNEventFile` connector, the HL7 messages are read from a disk. Reading messages from a disk is generally much faster than receiving them over a socket, so the `PollFrequency` and `PollQuantity` properties of the `HCNEventFile` connector should be used to control the rate at which messages are sent to the collaboration. Use the MQ Explorer to watch the number of messages on the queue `AP/HCNEventFileConnector/WebSphereServer`. If the number of messages is continually increasing (while messages are being read from the input file), then either the `PollQuantity` should be decreased or the `PollFrequency` should be increased to avoid having the queue exceed its maximum depth.

Also when using the `HCNEventFile` connector, the input directory should be on a physical disk drive which is not the same drive where the HCN Gateway and WebSphere Business Integration Server databases reside, to avoid disk contention which reduces the performance of the WebSphere Business Integration Server.

HCN subscriber gateway performance

The performance impacts of the HCN Subscriber Gateway are highly dependent on the customizations done on the gateway to receive publication messages and send them to the another application. The only general performance rule that applies is to pay attention to tuning the database and the database schema if the data from the messages are written eventually to a database.

WebSphere Business Integration server performance

For general information about tuning the WebSphere Business Integration Server, refer to *Introduction to WebSphere InterChange Server V4.2.2 Performance Tuning*, REDP-9124, which is available at:

<http://www.redbooks.ibm.com/abstracts/redp9124.html?Open>

HCN Message Flow server performance

The WebSphere Business Integration Message Broker, on which the HCN Message Flow Server is built, is a high performance message broker which can scale both vertically (by running on a wide range of hardware platforms) and horizontally (by clustering multiple instances of the Message Broker). Refer to the WebSphere Business Integration Message Broker product documentation for additional information.

There is an optional feature of the HCN Message Flow Server which allows you to keep a daily log on the file system of all publications sent through the Message Flow Server. If performance of the Message Flow Server becomes an issue, consider disabling the logging feature.

Database performance

The HCN Publisher Gateway, HCN Subscriber Gateway, and the HCN Message each utilize one or more DB2 databases to accomplish their work. Standard database tuning recommendations apply, although they are outside the scope of this Redbook. See the appropriate DB2 product manuals.

Abbreviations and acronyms

(ISC)²	International Information Systems Security Certification Consortium	HIPAA	Health Insurance Portability and Accountability Act
ADE	Adverse Drug Events	HL7	Health Level 7
AGPI	Anonymous Global Patient Identifier	HTTP	HyperText Transfer Protocol
AMI	Acute Myocardial Infarction	IBM	International Business Machines Corporation
ANSI	American National Standards Institute	ICD	International Classification of Disease
BSML	Bioinformatic Sequence Markup Language	ICD10	International Classification of Disease codes, version 10
CA	Certificate Authority	ICD9	International Classification of Disease codes, version 9
CAP	College of American Pathologists	ICL	Integration Component Library
CDA	Clinical Document Architecture	ICS	InterChange Server
CDC	Centers for Disease Control	IDN	Independent Delivery Network
CGv2	Clinical Genomics version 2 solution	ISO	International Organization for Standardization
CIS	Clinical Information System	ITSO	International Technical Support Organization
CISSP	Certified Information Systems Security Professionals	J2EE	Java 2 platform Enterprise Edition
CMS	Centers for Medicare and Medicaid Services	JAR	Java Archive
CPT	Current Procedural Terminology	JCE	Java Cryptography Extension
DASD	Direct Access Storage Device	JDBC	Java Database Connectivity
DDL	Data Definition Language	JMS	Java Message Service
EMR	Electronic Medical Record	LDAP	Lightweight Directory Access Protocol
FDA	Food and Drug Administration	LLP	Lower Layer Protocol
FTP	File Transfer Protocol	LOINC	Logical Observation Identifiers and Codes
GB	Gigabyte	MAGE-ML	MicroArray Gene Expression Markup Language
HCN	Healthcare Collaborative Network	MLLP	Mixed Low-level Protocol

NDC	National Drug Code
ODM	Operational Data Model for CDISC
OSI	Open Systems Interconnection
PHA	Public Health Alerts
QOC	Quality of Care
RAID	Redundant Array of Independent (or Inexpensive) Disks
SDO	Standards Developing Organization
SMTP	Simple Mail Transfer Protocol
SNOMED CT	Systematized Nomenclature of Medicine Clinical Terms
SOAP	Simple Object Access Protocol
SQL	Structured Query Language
SSL	Secure Sockets Layer
TCP/IP	Transmission Control Protocol/Internet Protocol
URL	Universal Resource Locator
VMD	Visual Message Definition
XML	eXtensible Markup Language
XPATH	XML Path Language
XSLT	Extensible Style Language Transformation

Related publications

The publications listed in this section are considered particularly suitable for a more detailed discussion of the topics covered in this redbook.

IBM Redbooks

For information about ordering these publications, see “How to get IBM Redbooks” on page 246. Note that some of the documents referenced here might be available in softcopy only.

- ▶ WebSphere Business Integration Adapters: An Adapter Development and WebSphere Business Integration Solution, SG24-6345-00
- ▶ Introduction to WebSphere InterChange Server V4.2.2 Performance Tuning, REDP-9124

Online resources

These Web sites and URLs are also relevant as further information sources:

- ▶ IBM WebSphere Business Integration for Healthcare Collaborative Network
<http://www-306.ibm.com/software/integration/hcn/>
- ▶ IBM WebSphere Business Integration for Healthcare Collaborative Network Gateway
<http://www-306.ibm.com/software/integration/hcng/>
- ▶ Evolution of the healthcare industry to a standards based environment: The impact on healthcare businesses
http://www-128.ibm.com/developerworks/websphere/library/techarticles/0407_schultz/0407_schultz.html
- ▶ IBM WebSphere Business Integration for Healthcare Collaborative Network information center
http://publib.boulder.ibm.com/infocenter/imshelp/v3r0/index.jsp?topic=/com.ibm.hcn.doc/install/c_insthub.html
- ▶ Foundation for eHealth Initiative - Healthcare Collaborative Network (HCN) community profile
<http://ccbh.ehealthinitiative.org/profiles/HCN.msp>

How to get IBM Redbooks

You can search for, view, or download Redbooks, Redpapers, Hints and Tips, draft publications and Additional materials, as well as order hardcopy Redbooks or CD-ROMs, at this Web site:

ibm.com/redbooks

Help from IBM

IBM Support and downloads

ibm.com/support

IBM Global Services

ibm.com/services

Index

A

- Administrative 129
 - Application 116
 - Messages 136
 - Server 7, 11, 37, 65, 68, 71–72, 82, 84, 99, 101, 104–105, 108, 114–115, 117, 123–124, 129, 141, 148, 208
 - Hardware requirements 52
 - Hints and tips 150
 - Planning 46
- Administrative server installation tasks 46
- Administrator 104
- Administrator task
 - creating a new organization 105
- Adverse Drug Event 10, 141, 143–145
- AGPI 8
 - Server 8, 16, 22–23, 33, 36–37, 47–48, 50–51, 64, 66, 70–71, 73, 78, 87, 95, 148, 162, 176, 214, 235
- AGPI server 70, 83
- American National Standards Institute 227
- Analysis 30
- Anonymous Global Patient Identifier
 - See also* APGI 8
- Apply new privacy code to collaboration 220
- Avian flu 10, 19, 24
- Avian influenza
 - See also* Avian flu

B

- Backup and recovery 162
- Binding the connector to a port 197
- Bioinformatic Sequence Markup Language 11, 146
- Bio-preparedness 6
- Bio-terrorism 2–3, 5–6
- Bird flu 17, 118–120, 145

C

- Certificate authority 59, 82
- Chameleon inbound equation 214
- Channels in the publishing Hospital WebSphere MQ Explorer console. 91

- Clinical topics 7–9, 141

- Attributes 9

- Collaboration

- HCN_EvaluateMessage 237–238

- Collaboration threading properties 240

- Connecting for Health 3

- Connector

- Connector Configurator 238

- controller 241

- delays 241

- HCNHL7 Connector 240

- Specific properties 238

- Connector Configurator 238

- Connector Configurator showing Poll Frequency 238

- Connectors 77–78, 155, 186–187

- CPT-4 123, 207

- Creating additional connectors 187

- Creating gateways

- required parameters 102

- Creating ICL project 184

- Creating new HCN connector 189

- Customization 13, 32, 38, 44, 181, 185–186, 189

- Customize the script used for privacy control 217

- Customizing HCN privacy rules 211

- cwservice command file 155

D

- Data interoperability 32

- Data review organization 4, 6, 8–11, 33

- Data source organization 4, 8, 33

- De-identification 98, 135, 167–171, 175–177, 211–212, 214, 217, 219, 221

- Deploy collaboration object. 199

- Description character error 122

- Disease outbreak 2, 5

- Display topics list 124

E

- Education planning tasks 44

- eHealth Initiative 3

- Example “start_WebSphereMQ_service.bat” file 156

Example of HCNSUB.PATIENT table content 96
Excerpt from Administrator's home page
create new user 108

F

Fix pack levels 66

G

Gateway 53, 151
Gateway hardware tasks 53
Gateway installation tasks 48
Gateway server 76
Gateway_to_Broker_CDAConstruktor 239
Gateway_to_Broker_Deidentification 239
Gateway_to_Broker_Evaluate 239
Gateways 33, 98, 101, 104
Creation 75, 110
Editing 112, 114
Installation 75
Managing 104, 110
Privacy levels 168–169, 171
Publisher 236
Tab 128, 134
User association 107
Viewing 128, 134
General hardware tasks 50

H

Haplotype Map 11, 146
Hardware requirements 65
HCN
Administrative server 10, 70, 73, 123, 143–144, 148–149, 173, 179
Application databases 162
Banefits
Data interoperability 12
Benefits 11
Participants 11
Clinical messages 8
Components 28, 30, 35–37, 39, 54, 57, 60, 63, 66, 82, 148, 159
Gateway 22–23, 37, 56, 66, 70, 75–76, 147, 152–153, 182, 188, 203, 222, 241
Hub 7–9, 15–16, 20, 22–23, 173, 178
Message Flow Server 147, 151, 173, 178, 188, 237, 242
Message flow server 8

Origins 3
Proof-of-concept 3–4
Spokes 8
Subscriber Gateway 242
Trends 5
Adverse drug reactions 6
Bio-preparedness 6
Cost reduction 6
Disease outbreaks 6
Maturity of technology 5

HCN Administrative server prerequisite software installation checklist 72
HCN configure and run 14
HCN connectors 187
HCN Entities and Core Functions 97
HCN hub and spoke structure 7
HCN privacy hierarchy 170
HCN system databases 163
HCN welcome page 81
HCN_Event 236
HCNBrokerConnector 78
HCNEventFile 236, 240
HCNHL7 236
HCNHL7Connector 240
HCNPubDB 237
HCNPubDBConnector 78
Health Level 7
See also HL7 225
Health topics 4, 118, 135
Creation 117, 124
Editing 124
Page 117
page 124
Tab 117, 124
Viewing 124
Healthcare ecosystems 3, 6, 11
HIPAA 13, 87, 169
HIPAAFullyDeidentified 21–24, 169, 212
HIPAALimitedDataSet 21–25, 169, 212
HL7 6, 8–10, 22–23, 25, 32, 34, 77, 93–95, 115, 122, 143, 168, 171, 174–178, 188, 190, 194, 200, 203, 205–206, 211–212, 215, 221–223, 227, 236
Clinical Document Architecture 9, 122, 233
Connector 179
LLP Connector 188
Message security 233
Message structure 228
MLLP 188–189
MSH segment 233

- Simulator 199, 201
- Structure of messages 230
- Toolkit 218
- Types of messages 231
- HL7 LLP Connector 188
- HL7 Message evaluation flow 236
- HL7 message structure artifacts 229
- HL7ResponseDelayWhenCongested 241
- Hospital_to_Gateway_AGPI 239
- Hospital_To_Gateway_Entry 196, 239
- Hospital_to_Gateway_Entry 198–199
- How HCN Works 6

I

- IBM 3–4, 30, 44
 - Aligned Clinical Environment 3
 - Clinical Genomics 122, 146, 221, 233
 - DB2 UDB Universal Database Express 74
 - DB2 UDB Workgroup Server 71–72
 - DB2 Universal Database 46
 - DB2 Universal Database Express 49, 70
 - DB2 Universal Database Workgroup Server 47–48, 67–68
 - Tivoli Directory Server 46, 69, 72, 149
 - WebSphere Application Server 46, 68, 72, 148, 173
 - WebSphere Business Integration 1–2, 4, 34, 63, 72–73, 75, 77, 97, 104
 - Adapter for JDBC 49, 70
 - Adapter for JText 49, 70
 - Adapter for web services 49, 70
 - Adapter for WebSphere MQ 49, 70
 - Message Broker 68, 71
 - Server Express 49, 66, 70, 74
 - WebSphere Business Integration Message Broker 47
 - WebSphere MQ 46–49, 66, 68, 70–72, 74, 173
- ICD-9 6, 123, 143, 207
- IKeyman tool
 - creation of hospital publisher gateway key data-base file 84
- Information flow in HCN 172
- Installation 19
 - Configuration 13
 - HCN 58
 - Pre 29
 - Requirements and prerequisites 64
 - Solution overview 64

- Validation 87
- WebSphere Business Integration Server 75
- installation 13
- Installation and configuration 63
- Integration component library 183
- InterChange server component manager 182
- International Organization for Standardization 226
- Introduction to Healthcare Collaborative Network 1
- ITSO HCN Public Health Alert scenario physical layout 88

J

- JDBC Connector 188
- JText Connector 188

L

- LOINC 6, 123, 207

M

- Managing organization list 106
- Managing topics 117
- MaxMessageQueueDepth 241
- Message Flow server 65, 67, 71, 82
 - See also* HCN Message Flow server
- Message Flow Server installation tasks 47
- MicroArray Gene Expression Markup Language 11, 146
- Modifying or extending the pre-defined codesets 207

N

- New self signed certificate properties 85
- Notification 93, 136, 139, 150, 171
 - Administrative Server 136
 - Confirmation 138
 - Creation 137
 - E-Mail 70, 75, 89, 136, 150
 - Tab 137–138
- Notifications 138

O

- Observer 40, 93, 103–104, 114, 129, 134
- Open Systems Interconnection 226
- Operational Data Model 11, 146
- Organization details 107
- Organization list 100
- Organizations 33, 98–99

- Creation 93, 105
 - Managing 104–106
 - Privacy levels 168
 - Tab 100
- P**
- PatientID 95, 229
 - Performance
 - Database 242
 - Gateway connector 240
 - HCN Message Flow server 242
 - Publisher gateway 236
 - Subscriber gateway 242
 - WebSphere Business Integration server 242
 - Performance tuning 235
 - Planning
 - Administrative server 46
 - AGPI server 47
 - Education 42
 - Gateway 48
 - Hardware 49
 - Hub 51
 - Message Flow Server 46
 - Networking 54
 - Windows OS 45
 - Planning and design 27
 - Planning and design (L) V 27
 - Planning for data interoperability 55
 - Planning for education 42
 - Planning for software 45
 - Poll frequency 237–238
 - Polling 236
 - Polling interval 237–238
 - Preparing HCN development environment 182
 - Primary user 33, 40, 75, 93, 98–99, 103–105, 112
 - Gateway 22–23, 136
 - Organization 21–22
 - Privacy and security 165
 - Privacy and Security in our scenario 174
 - Privacy level 9, 21–22, 25
 - Gateway 22–24
 - Privacy levels 33, 98, 135, 168–169, 211
 - Application 170–171
 - Customization 212
 - Dependency 169–170
 - Editing 219
 - Privacy processing in HCN 171
 - Public Health Alert 10, 17, 25, 87, 92–93, 118–119, 141, 145, 174
 - Our scenario 18
 - Stages of pandemic 17
 - Public Health Alert scenario 17
 - Publication Details page 131
 - Publisher 135
 - Gateway 15
 - Publisher Gateway 8–9, 22–23, 78–79, 83, 101, 114, 122, 151, 159, 168, 170, 175, 177–178, 188, 219, 221, 233, 236, 242
 - Python 32, 48, 70, 74, 205, 212–214, 217, 219, 222
 - python 219
- Q**
- QOC
 - See also* Quality of Care 19, 24, 141
 - Quality of Care 10, 19, 24, 141–142
- R**
- Redbooks Web site 246
 - Contact us xiv
 - Review the ICL components 186
- S**
- Sample cwservice invocation 157
 - Sample Influenza_A_H5N1 topic parameters 25
 - Sample Python code for privacy control 213
 - Security 33
 - Segment grammar 206
 - server 129
 - SMTP server 75, 87, 150
 - Software prerequisites 66
 - Solution models 15
 - Academic Medical Research Center 15
 - Government Sponsored 15
 - Independent Delivery Network 15
 - Regional Health Collaboration 15
 - Sole Subscriber 16
 - Solution overview 2
 - Solution plans 42
 - Solution scope
 - Data interoperability 29
 - Deployment 29
 - Number of site 29
 - Topics 29
 - User roles 29
 - Users 29

- Solution stages 28
 - Installation 36
 - Components installation 37
 - Configuration 38
 - Prerequisite software 36
 - Post installation 39
 - Availability and continuity 42
 - Solution roll out 41
 - Solution Validation 39
 - System management 42
 - User training 40
 - Pre installation
 - Analysis 30
 - Solution design 32
 - Solution plans 35
 - Solution scope 29
- Standards Developing Organization 227
- Start HCN server batch file 153
- Subscriber 135
 - Gateway 8, 15
- Subscriber Gateway 33, 37, 40, 83, 92, 94–95, 101, 107, 111, 114, 122, 134–135, 142, 159–160, 162, 170, 174, 188, 242
- Subscriber gateway MQCONN.ARCHIVE queue 94
- Subscriber Gateway queues in the ACD institution. 92
- System log files 148
- System Management 147
- System management 147
 - Administrative Server
 - LDAP administration 149
 - Log files 148
 - Gateway
 - Log files 151
 - Gateway tracing 157
 - Message Flow Server
 - Log files 151
 - WebSphere MQ Queues 159
 - Gateway archive queues 159
 - WebSphere MQ troubleshooting 160

T

- The hub 33
- The scenario
 - Communication 19
 - Health system response 19
 - Organizations 20

- HCN Central 20
- ITSO Hospital 21–22
- ITSO Lab 22
- Public Health Alert 18
- Publishers 22
- Subscribers 23
- Surveillance 19
- Topics 24
- Topic creation screen 24
- Topics 34
 - Managing 104

U

- User roles 98, 104
- User roles and administration 97
- User skills 31
- Users 33, 103, 137, 170
 - Association to Gateways 108
 - Creation 108
 - Managing 104, 107
 - Organization association 105
 - Page 108–109
 - Privacy 166
 - Tab 108

V

- Validating user input 123

W

- WebServices Connector 188
- WebSphere 91
- WebSphere Business Integration 192, 242
 - Message Broker 47–48
 - Server Express 151
 - Toolset 182, 186
 - Workbench System Manager 219
- WebSphere Business Integration Interchange Server 76
- WebSphere Business Integration Server 182
 - Performance 239
- WebSphere Interchange system log file 152
- WebSphere MQ 39, 46–47, 49, 66, 77, 80, 159, 161, 178
 - Adapter 70
 - Channels 79
 - Cluster 91
 - Configuration 89

Explorer 90–91
Fix packs 70, 72
Queues 147, 159, 188
SSL 82, 86
Troubleshooting 160
WebSphere MQ queues and Queue Managers 159
WebSphereMQ Connector 188

X

XML

 messages,incoming 236
XML Only Contents 141



Healthcare Collaborative Network: Solution Planning and Implementation

(0.5" spine)
0.475" <-> 0.875"
250 <-> 459 pages



Redbooks

Healthcare Collaborative Network

Solution Planning and Implementation

Plan and design interconnected healthcare information solutions

The IBM WebSphere Business Integration for Healthcare Collaborative Network is an internet-based, private information network that enables secure transmission of clinical data to healthcare participants.

Install and configure Health Collaborative Network components

Healthcare Collaborative Network enables immediacy in the dissemination of clinical data and provides participants with capabilities to detect and respond rapidly to health risks such as adverse drug effects, to manage quality of care, and to implement monitoring and warning systems for detecting the onset of dangerous infectious diseases or bioterrorist attacks.

Get started with a Public Health Alert example

This IBM redbook provides a first-hand guide for creating solutions based on the IBM WebSphere Business Integration for Healthcare Collaborative Network. It includes an example scenario of a public health alert based on Avian Influenza (bird flu) and Avian Influenza A (H5N1).

Healthcare Collaborative Network is aimed at hospitals and large groups of medical or dental practices, international and government agencies, pharmaceutical companies, and major insurance companies.

**INTERNATIONAL
TECHNICAL
SUPPORT
ORGANIZATION**

**BUILDING TECHNICAL
INFORMATION BASED ON
PRACTICAL EXPERIENCE**

IBM Redbooks are developed by the IBM International Technical Support Organization. Experts from IBM, Customers and Partners from around the world create timely technical information based on realistic scenarios. Specific recommendations are provided to help you implement IT solutions more effectively in your environment.

For more information:
ibm.com/redbooks