



iWay Software: HIPAA Solutions – and Beyond

A White Paper



Table of Contents

1	Introduction
3	HIPAA – A Business Challenge and Opportunity
4	The Path to HIPAA Compliance
<u>4</u>	HIPAA Education
<u>4</u>	Gap Analysis and Documentation
<u>4</u>	Risk Assessment
<u>4</u>	Policy and Procedure Development
<u>4</u>	Policy and Procedure Enforcement
5	The Role of Information Technology
6	Unique HIPAA Challenges for Information Technology
7	iWay Software Solutions for HIPAA Compliance
<u>7</u>	Comprehensive Support for Complex Business Requirements
9	Why iWay Software and Information Builders?
<u>9</u>	The Bottom Line
10	Appendix – Just What Is “HIPAA Certification”?
<u>10</u>	Overview of the Six Levels of Testing Necessary for HIPAA Transaction Certification – as Recommended by WEDI.SNIP
<u>10</u>	Level 1 – Integrity Testing
<u>10</u>	Level 2 – Requirement Testing
<u>11</u>	Level 3 – Balancing
<u>11</u>	Level 4 – Business Scenario “Situational” Testing
<u>13</u>	Level 5 – Codes and Volumes
<u>13</u>	Code-Set Testing
<u>14</u>	Load/Capacity/Volume Testing
<u>14</u>	Level 6 – Services and Security
<u>14</u>	Product Types/Types of Service Testing
<u>14</u>	Security/Privacy

Introduction

The Health Insurance Portability and Accountability Act (HIPAA) was enacted in 1996 and includes provisions for the following improvements in the U.S. Healthcare system nationally:

1. Assurance of the portability of health plan coverage
2. Limitations on how pre-existing condition restrictions can be applied
3. Strict protections of a patient's right to privacy and confidentiality
4. Administrative simplification to reduce non-clinical healthcare operating costs

The impetus behind the fourth requirement was no less than the federal government's objective of balancing the federal budget and the reduction of its spending deficit. HIPAA would help support this macroeconomic objective, theoretically, by mandating the use of standards whenever healthcare entities send automated transactions to one another. That of course includes any entity doing business with HCFA's (Health Care Financing Administration) healthcare agencies – Medicare and Medicaid. And, indeed, these two entities account for a mammoth portion of the federal budget. As well, nearly every healthcare organization in the United States does business with these two government sponsors of health coverage.

Accordingly, any streamlining of businesses-to-business communications and related processes would in theory provide an operational cost savings to – among others – the federal government's healthcare branches. This is but one factor that has catalyzed a push for HIPAA enactment and enforcement.

To make HIPAA work, the secretary of the Department of Health and Human Services was required to adopt standards to support the Electronic Data Interchange (EDI) of administrative and financial healthcare transactions primarily between healthcare providers and plans. And, as most know, the choices were:

- ANSIX12 for EDI in Healthcare
 - October 1997 ASC X12 Standards Version 4, Release 1, Sub-release 0 (004010)
- NCPDP for EDI Specific to Retail Pharmacies
 - NCPDP, Real-Time Transactions Version 5.1
 - NCPDP, Batch Transactions Version 1.0
- Adoption of various medical and nonmedical code sets to be used in conjunction with these standards

What's more, the provisions for administrative simplification include the use of national identifiers for the key entities in healthcare:

- Payers
- Employers
- Providers
- Patients

The nomenclature and for these identifiers has yet to be agreed upon.

Lastly, the provision for protections of a patient's right to privacy and confidentiality has been only vaguely defined in terms of precisely how that should be achieved when information technology (IT) is involved.

So, to say the least, HIPAA mandates present both business and information technology challenges. The purpose of this white paper is threefold:

1. To explore the role of emerging technologies and solutions that best support a healthcare organization in its efforts to achieve compliance with the HIPAA mandates for standardized EDI
2. To describe how those information technologies can also support healthcare organizations' efforts to quickly and fully achieve certification for HIPAA compliance in areas of business processes
3. To describe the business value these information technologies, when used appropriately, can provide an organization as they form the foundation for process improvements and cost management that go well beyond the initial objectives of achieving HIPAA compliance

HIPAA – A Business Challenge and Opportunity

We have all heard analogies between HIPAA and Y2K. For one thing, expenditures for HIPAA are projected to exceed those of Y2K. Also, Y2K arguably did not offer any business advantages or return on investment. However, with HIPAA, IT enhancements necessary for compliance also promise to become driving forces in reducing costs in healthcare and may even be found to help improve aspects of patient care quality.

Achieving HIPAA compliance requires enormous resources, both financial and fiscal. Healthcare organizations must derive as much benefit as possible from this investment. If they can capitalize on HIPAA spending, they can leapfrog other organizations that merely seek to meet the letter of the law, and become more efficient, flexible, and profitable.

The rampant use of proprietary formats for handling healthcare information within and among self-developed and vendor applications has led to increased administrative costs and complexities for healthcare organizations: thus, a challenge – and opportunity.

By redesigning business and technology processes, healthcare entities are looking to achieve compliance with HIPAA mandates. Yet, there are clear opportunities to:

- Improve operational efficiencies and reduce costs
- Avoid costly replacements of existing systems – leveraging investments in these systems by using tools to assure their compliance with HIPAA mandates for standardized transactions
- Provide absolutely secure and appropriate access to strategic, clinical, and other key information

The Path to HIPAA Compliance

Achieving HIPAA compliance involves five distinct phases:

HIPAA Education

Some companies are still involved in this phase. Advice regarding obligations, policies, and procedures is most important for those educating themselves about HIPAA. Technology education is important in that administrators need to understand what technology can and cannot do for them.

Gap Analysis and Documentation

Gap analysis is the phase in which existing policies and procedures are analyzed in the light of HIPAA regulations. Organizations identify and document weaknesses in current policies or their enforcement. Legal, medical, and financial staff is useful in this phase. In addition, technology must be assessed for compliance and non-compliance, options laid out for remediation (e.g., replace, re-engineer, enhance with adapters and toolsets, etc.), and costs for those options – as well as return on those investments – have to be ascertained.

Risk Assessment

Gaps identified in gap analysis and documentation have different risk levels. Risk assessment categorizes gaps according to fiscal, legal, and medical priority in order to manage policy and procedure development and enhancement. This should be a business-oriented risk assessment, that would include a risk/reward assessment of the IT options for remediation. The types of technologies that could mitigate these risks should all be explored for feasibility and cost effectiveness. Yet, projects should not be planned solely on the basis of available technology. Rather, they should be based first on business requirements.

Policy and Procedure Development

This is a natural outgrowth of risk assessment, in that each policy and procedure should be traceable to specific gaps with a priority based on the risk assessment. Although organizations should develop policies and procedures according to business needs, they should begin to consult with Information Technology staff and vendors to ensure that policies and procedures are enforceable through off-the-shelf technologies and highly adaptable toolsets that are designed, engineered, and configured to meet HIPAA related – and indeed general healthcare IT – requirements.

Policy and Procedure Enforcement

Once organizations have determined the policies and procedures that they will follow, they must look at the infrastructure that will support them. At implementation time, Information Technology staff and vendors are heavily involved in developing computer systems that automate the management, monitoring, and auditing of the policies and procedures developed in policy and procedure development.

The Role of Information Technology

Technology may not help organizations develop policies and procedures, but it can be used as a tool to enforce them without significant impacts to the organization. Trusted vendors can provide advice in this regard. Examples may include:

- Ability to meet at levels 1-5 of the WEDI SNIP structured HIPAA Certification Process. (See Appendix – Just What Is “HIPAA Certification”? on page 11.) For instance, a best-of-breed EDI platform would:
 - Assure an organization sends an ANSI X12N EDI transaction with integrity and validity (level 1)
 - Yet, it would also perform transaction balance checks and assure the use of appropriate medical code sets (levels 4 and 5) through the use of a rules engine
- Support for enveloping transactions with the highest levels of security possible – all to assure patient privacy and confidentiality is protected
- Track and audit information access; provide authentication and nonrepudiation of service
- Improve patient care by providing caregivers (with appropriate authorization) secure and situational access to patient data via external communication technologies such as Web pages, XML documents, and EDI

Once policies have been put in place, the purpose of information technology is to automate and enforce the policies that have been created by the business units. It is critical that these technology solutions provide the privacy, security, and adherence to standards required by HIPAA legislation.

Unique HIPAA Challenges for Information Technology

HIPAA legislation demands that all healthcare organizations use specific transactions to interact with other healthcare organizations. Yet most healthcare organizations do not want to disrupt their current operations by buying completely new information systems that natively support these transactions. For that matter, they may not want to incur the cost and risk of upgrading existing systems unless necessary. So IT can help manage the risk of HIPAA compliance by integrating existing systems rather than upgrading old ones or buying new ones.

In addition, all of these transactions should be for as many uses as possible in order to derive maximum benefit from them. For example, a hospital's business-to-business (B2B) initiative that uses EDI transactions should also have the flexibility to make the same transactions available using XML – not because the hospital needs XML-based transactions right now, but because many organizations are moving to XML as an integration technology. This is true regardless of the buzzwords and standards being used. Ultimately, organizations will need to make transactions open to authorized practitioners, insurance companies, government compliance oversight agencies, patients, and their own internal users.

In addition, no organization will want to have several solutions to achieve the same objectives in different areas of their operation. For instance, one integration engine solution should be robust enough to manage not only HIPAA-mandated EDI transaction set standards, but should also support integration between HL7-compliant and noncompliant systems.

All aspects of HIPAA-compliant systems must provide security and privacy measures. This is particularly important for transaction processing and information delivery (reporting), since these are the most common ways of interacting with information systems on a large scale. Platforms for transaction processing and information delivery must respect existing security in existing systems' transactions and databases.

iWay Software Solutions for HIPAA Compliance

Comprehensive Support for Complex Business Requirements

iWay Software and its parent company, Information Builders, understand. We have a 26-year history of delivering pragmatic software solutions to significant business problems, and many healthcare companies have placed their trust in us. We can help you manage and improve your HIPAA compliance efforts with software and services that provide solutions for secure, reliable, and flexible business integration and information delivery.

iWay Software is a leading provider of integration software. The iWay Enterprise Integration Suite lets you use existing information systems in new ways that help you comply with HIPAA regulations. By restructuring and automating your business processes, iWay makes it easier to enforce policies with the level of reliability, security, and availability that your organization needs.

iWay specifically provides:

- Built-in support for the EDI transactions that HIPAA requires (ANSI and NCPDP)
- Capabilities to support HL7 and non-HL7 messaging and systems integration
- Integration and rules-based tools that help automate and enforce business processes
- Nearly codeless integration capabilities that reduce the amount of knowledge and effort required by your IT staff
- Point-and-click tools that dramatically reduce the amount of customization needed for a given solution

Information Builders, iWay Software's parent company, is a leading provider of information delivery software. Information Builders' WebFOCUS lets you disseminate and analyze information in a secure, auditable, and flexible way that can ensure correct information disclosure to patients, practitioners, insurance companies, and government agencies.

These comprehensive software products are backed by Information Builders Professional Services, a worldwide organization that specializes in the rapid integration of complex information systems for enterprise applications and information delivery.

iWay has a powerful combination of integration and data extraction tools that – together – can be used to achieve HIPAA compliance and to improve business performance. Several examples follow:

- A hospital may select a vendor of security software to provide secure transmission of a report. This security vendor is not likely to provide a way to read information from the hospital's applications and format it into the report. The hospital can select an information delivery product, like Information Builders' WebFOCUS, that is compatible with this vendor's security software. Together, they provide a HIPAA-compliant reporting system.
- The same hospital, when it chooses an enterprise application integration (EAI) tool, may look for a product like iWay Software's Enterprise Integration Broker, which is compatible with the software from both the security vendor and the reporting vendor.
- Some tools will provide additional capabilities that complement another vendor's capabilities. For example, although Information Builders is not a security company, it provides unique tools to audit the way that iWay and WebFOCUS products access data and applications.

Why iWay Software and Information Builders?

The stability and reliability of iWay Software and Information Builders make it a very attractive choice in these turbulent times. But there are additional reasons to entrust the IT aspect of HIPAA compliance to us.

1. We have a deep and long-term understanding of healthcare through our extensive client base.
2. We have long experience with complex integration tasks for reporting and operations.
3. We have the deepest and broadest expertise with legacy systems of any vendor on the market.
4. We are able to use these legacy systems with cutting-edge technologies and standards to help provide a flexible and powerful infrastructure.
5. We can provide software and personnel from a single organization to manage a significant portion of your IT requirements resulting from HIPAA legislation.
6. We can also work with specialized partners, including both Big 5 consulting firms and small boutique companies.
7. We are completely vendor-neutral, so you are not locked into the proprietary solutions of a single vendor. We can work with other vendors' products if you already have them, or supply an end-to-end solution.
8. We are not tied to any particular application company, providing a flexibility and independence that most application vendors lack.
9. Our software will still be useful after your next merger because of the breadth of capabilities, level of interoperability, and flexibility that we provide.
10. We have over 25 years of integration experience in healthcare, financial services, and other vertical markets, which have gone through these types of integration challenges before.

The Bottom Line

iWay Software has the tools, people, and experience to turn a compliance nightmare into a new opportunity for you to differentiate yourself from your competition.

Learn how to take commodity IT systems (i.e., those that everyone has), custom or customized "keystone" systems (i.e., those that set you apart), your existing personnel, and a little help from iWay Software, and turn them into a world-class, fully integrated, strategically oriented information infrastructure that can support your employees, patients, and partners better than ever before. You'll get better risk management, higher profits, and contained costs.

Appendix – Just What Is “HIPAA Certification”?

Overview of the Six Levels of Testing Necessary for HIPAA Transaction Certification – as Recommended by WEDI.SNIP

The following compilation summarizes the various descriptions given by WEDI (Workgroup for Electronic Data Interchange) for the levels of certification testing a healthcare organization would need to successfully pass in order to have that organization recognized as compliant with the HIPAA mandates for sending ANSI X12N Standardized Transactions to its trading partners. (Extractions of the two source documents from which this compilation derives are appended to this document.)

An EDI transaction translation system utilized by a healthcare organization must be fully supportive of that organization’s efforts to pass these levels of certification – most directly supportive at levels 1 and 2; and, indirectly at levels 3-6.

Level 1 – Integrity Testing

This level of testing involves making certain the EDI transaction translation system will import an EDI transaction – regardless of format – and export the transaction with valid EDI files and with full data integrity. This must be a repeatable test with all nine X12 transaction sets.

This is to say that the EDI transaction translation system must accept an incoming EDI transaction, regardless of format, and reformat the record and export it so it contains valid segments, segment order, and element attributes. For instance, there must be numeric values in numeric data elements. This level of testing will validate complete adherence and compliance with the ANSI X12N, Version 4010 standard’s syntax and rules as mandated by the HIPAA regulations. This first level of testing will validate the most basic level data integrity for the EDI submission.

Level 2 – Requirement Testing

This level of testing, and in particular succeeding levels of testing, will be structured according to the frameworks described in the HIPAA Implementation Guide. For instance, the specific requirements called out in the implementation guide include:

- Testing for implementation guide-specific required data elements and segments; for example:
 - Repeat counts
 - Required or intrasegment situational data elements
- Testing for valid code values noted in the implementation guide via an X12 code list or table. However, at this level of testing, there is no need to test the logic of using a certain code within the context of the transaction type of values within the transaction. Items to consider include the following:
 - Used and unused codes

- Testing for nonmedical code sets. Examples of nonmedical code sets include the following:
 - Zip code
 - Countries – ISO 3166
 - Currencies and funds – ISO 4217
 - D-U-N-S number
 - Universal product code
 - Etc.
- Testing and validation of any mandated medical code set values. Examples of medical code sets include the following:
 - CPT-4 (Current Procedural Terminology)
 - ICD-9-CM (International Classification of Diseases – 9th Revision – Clinical Modification)
 - ICD-10-CM (International Classification of Diseases – 10th Revision – Clinical Modification)
 - DRG (Diagnosis Related Group)
 - NDC (National Drug Code)
 - Etc.

Level 3 – Balancing

Testing the transaction for balanced field totals, record or segment counts, financial balancing of claims or remittance advice, and balancing of summary fields, if appropriate.

For example, with respect to the Healthcare Claim Payment/Advice (835) transaction, there are three fields that must total to the correct value, i.e.:

Service Payment Information (segment SVC02)

(Charge submitted during claim for service rendered)

+/- Service Adjustment Information (segment CAS_n)

(Modification by payer (may be based on pre-negotiated fees))

Service Payment Information (segment SVC03)

Level 4 – Business Scenario “Situational” Testing

This level of testing takes business rules into account to a much greater degree than the first three levels of testing. The focus is on the nature of the relationship trading partners have that send EDI transactions to one another. WEDI.SNIP contends that this level should be well documented.

The reason this level of testing – and those which follow – are so much dependent on business rules and business processes is the requirement that HIPAA Transaction Set Testing must assure there is adequate data in an EDI transaction to perform a specific set of business functions and procedures. For instance, there must be sufficient information in an 837 (claim submission by a provider to a payer) so that the payer can accurately and appropriately adjudicate the claim.

Nonetheless, it is clearly stated by WEDI.SNIP that the modus operandi the payer employs (to use this example) in adjudicating a claim is not within the purview of HIPAA Testing. Testing scenarios cited by WEDI.SNIP for this level of certification include the following:

Conditional Situations

The testing of specific intersegment situations described in the HIPAA implementation guides, such that: If A occurs then B must be populated. This is considered to include the validation of situational fields given values or situations present elsewhere in the file.

Example 1: Health Insurance Eligibility Verification Request for Covered Benefits (270) transaction:

An information source must support a generic request for Eligibility. This is accomplished by submitting a Service Type Code of “30” (Health Benefit Plan Coverage) in the “EQ” loop of the transaction.

Example 2: Health Care Claim or Equivalent Encounter Information and COB (837) transaction:

If the claim is for an accident, the accident date must be present.

Code Sets

Whereas the WEDI.SNIP “Testing and Certification” document suggests this is to be tested at Level 4, its “Business-to-Business Transaction Set Testing” document as well as Claredi’s documentation suggests code-set testing would take place at Level 5. Thus, please refer to Level 5 below for this testing modality.

Product Types or Types of Services

Whereas the WEDI.SNIP “Testing and Certification” document suggests this is to be tested at Level 4, its “Business-to-Business Transaction Set Testing” document as well as Claredi’s documentation suggests code-set testing would take place at Level 6. Thus, please refer to Level 6 below for this testing modality.

Partner Data Validation

This would apply when testing transactions to and from a trading partner. (Please note that the term "trading partner" is synonymous with "business partner.") While lower levels of testing assuring data values and formats are valid per the X12 format, this level of testing would additionally assure that the transaction and data within it are valid for the particular business partnership being tested and would be contained within the business partner's database.

Example: Level 2 testing could verify that a provider number was of the proper format (10-position numeric), while this level of testing would verify that the provider number was actually in the payer's database.

Field Lengths

There are some fields that have very long maximum lengths in the X12 standard, where the Business Partner's system may not be able to accommodate fields at or near these maximum lengths. HIPAA rules prohibit the rejection of a transaction when they follow the X12 standards, but if a Business Partner's system is continually truncating specific fields, adjustments may need to be made. Thus, an effort must be made to diagnose and correct this problem and a reasonable effort made to remediate it through a combination of agreed to procedural and technical solutions.

Output

Checking to be certain EDI transactions can be produced by the sending entity are in keeping with the nature of the partnership and in keeping with the requirements of the receiving entity.

Example: A provider may wish its payer trading partner to submit certain transaction types via fax (which would be in keeping with HIPAA guidelines since it would not be considered an EDI transaction)

Level 5 – Codes and Volumes

Testing Code Sets and Load/Capacity/Volume

This level reviews testing two capabilities: the use of appropriate code sets, and assurance that the sending and receiving systems can accommodate the same transaction set capacities (the ability to accept transaction record sizes and transaction volumes).

Code-Set Testing

Whereas Level 2 testing focuses on valid code values as noted in the implementation guide X12 code list, this level of testing assures testing for valid implementation guide-specific code set values. That is, this level of testing will not only validate the code sets but also make sure the usage is appropriate for any particular transaction. The testing validates external code sets and tables such as CPT, ICD9, CDT, NDC, status codes, adjustment reason codes, and their appropriate use for the transaction.

Example: A CPT code (for outpatient care) should not be used for a claim transaction sent on an inpatient episode of care.

Load/Capacity/Volume Testing

Testing to ensure that the systems of each of the Business Partners will not fail because of increased file sizes or transaction volumes. Partners should agree on these factors in their relationship agreements. Once completed, they should test by simulating the volume of transactions that they estimate will be processed in the production environment. This is particularly important since the X12 transactions can be quite large. Examples of aspects that should be checked are temporary file space, batch run times, and capacity of translators or other front-end programs.

Level 6 – Services and Security

This level reviews testing two capabilities: testing that transactions are appropriate for the nature of clinical service provided (or health plan "product" or coverage), and assurance that the sending and receiving systems will take all reasonable and appropriate measures to ensure that the transaction is secure and, thus, the confidential nature of its content is maintained and patient privacy protected.

Product Types/Types of Service Testing

Testing at Level 6 is required to ensure that the segments and data within the EDI transaction are appropriate for the specific provider type that generates the transaction. That is, the data must be appropriate for the provider – whether it is a hospital, physician practice, dental practice, ambulance service, home health or other long-term care, durable medical equipment supplier or distributor, psychiatric facility, and other specialized services. These and all provider types have specific requirements that must be tested before putting the transaction into production.

Security/Privacy

Testing at this level must ensure that specific processes and technologies are in place between business partners to make sure that the security, privacy, and confidentiality of all patient data is kept.

The HIPAA regulations – and interpretations made by various advisory bodies – all agree that every effort must be made to ensure the protection and security of Patient Identifiable Information sent via EDI transactions. While it would be ideal to be able to reference an existing security and privacy methodology (i.e., standards, technological frameworks, security heuristics, etc.) as might be defined under HIPAA – such definition has yet to be agreed to within the industry or enacted by law. Thus, the prevailing wisdom in the industry is to take all reasonable available measures to protect patient privacy. The most common approaches considered to date are the most widely accepted in the IT industry as a whole. These include the use of secure connectivity (VPN versus internet), encryption/decryption (128 bit), public key/private key, and procedural controls.

WEDI.SNIP's Testing Sub Work-Group White Paper, "Testing and and Certification."

WEDI.SNIP's Transaction Testing Sub Work-Group White Paper, "Business-to-Business Transaction Set Testing."

Sales and Consulting Offices

- **Atlanta**, GA (770) 395-9913
- **Baltimore**, MD Consulting: (703) 247-5565
- **Boston**, MA (781) 224-7660
- **Charlotte**, NC Consulting: (704) 334-7440
- **Chicago**, IL (630) 971-6700
- **Cincinnati**, OH (513) 891-2338
- **Cleveland**, OH (216) 520-1333
- **Dallas**, TX (972) 490-1300
- **Denver**, CO (303) 770-4440
- **Detroit**, MI (248) 641-8820
- **Federal Systems**, DC (703) 276-9006
- **Hartford**, CT Consulting: (860) 249-7229
- **Houston**, TX (713) 952-4800
- **Kansas City**, MO (816) 471-3320
- **Los Angeles**, CA (310) 615-0735
- **Metropolitan**, NY Sales: (212) 736-7928
Consulting: (212) 736-4433, ext. 4443
- **Milwaukee**, WI Consulting: (262) 827-4685
- **Minneapolis**, MN (612) 338-5181
- **New Jersey** (973) 593-0022
- **Orlando**, FL (407) 804-8000
- **Philadelphia**, PA (610) 940-0790
- **Pittsburgh**, PA (412) 494-9699
- **Sacramento**, CA Consulting:
(916) 973-9511
- **St. Louis**, MO (636) 519-1411
- **San Jose**, CA (408) 453-7600
- **Seattle**, WA (425) 861-9400
- **Washington**, DC Sales: (703) 276-9006
Consulting: (703) 247-5565

Subsidiaries

- **Australia** Information Builders Pty. Ltd.
Melbourne 61-3-4631-7900
Sydney 61-2-8234-0600
- **Belgium** Information Builders Belgium
Brussels 32-2-7430240
- **Canada** Information Builders (Canada) Inc.
Montreal (514) 630-1134
Toronto (416) 364-2760
Vancouver (604) 688-2499
Victoria (250) 995-8622

- **France** Information Builders France S.A.
Paris 33-14-507-6600
- **Germany** Information Builders (Deutschland)
Dusseldorf 49-211-522877-0
Eschborn 49-61-96400804
Munich 49-89-354890
Stuttgart 49-711-72-87-28-80
- **Netherlands** Information Builders
(Netherlands) B.V.
Amsterdam 31-20-4563333
- **Portugal** Information Builders Portugal
Lisbon 35-121-726-90-11
- **Spain** Information Builders Iberica S.A.
Madrid 349-1-7102275
- **Switzerland** Information Builders
Switzerland AG
Wallisellen 41-1-8394949
- **United Kingdom** Information Builders
(UK) Ltd.
London 44-208-9824700
Warrington 44-1925-820111

Representatives

- **Argentina** Ditra S.A.
Buenos Aires 54-114-3071850
- **Austria** FOCUS Software Consult
Vienna 43-1-211363870
- **Brazil** Information Management Ltda.
Rio De Janeiro 55-21-2397755
Sao Paulo 55-11-2536303
- **Egypt** Standardata, Cairo 202-4183374
- **Finland** InfoBuild Oy
Helsinki 358-9-3433400
- **Gulf States** ■ Bahrain ■ Kuwait ■ Oman
■ Qatar ■ Saudi Arabia ■ Yemen
■ United Arab Emirates
Al-Gosaibi Information Systems
966-385-745-55
- **Hong Kong** Interim Technology
Hong Kong 852-2834-4788
- **Ireland** ACSIS Technologies (Ireland) Ltd.
Dublin 353-1-8725233

- **Israel** NESS A.T. Ltd.
Tel Aviv 972-3-5483555
- **Italy** Selestia G C Applications S.P.A.
Milan 39-02-2515181
Rome 39-06-729-018-28
- **Japan** K.K. Ashisuto
Osaka 81-6-373-7113
Tokyo 81-3-3437-0651
- **Korea** Unitech Infocom Co. Ltd.
Seoul 82-2-3477-4456
- **Mexico** Selestia Mexico S.A. de C.V.
Mexico D.F. 525-254-5050
- **Norway** iSolutions AS
Stavanger 47-51-4447-44
- **Singapore** Interim Technology
Singapore 65-2255077
- **South Africa** International Computers
S.A. (Pty.) Ltd.
Johannesburg 27-11-2335911
- **Sweden** Cybernetics Business
Solutions AB
Solna 46-8-470-378-00
- **Taiwan** Galaxy Software Services
Taipei 886-22-3897722
- **Turkey** Istanbul
Information Builders 90-212-335-2745
Key Soft Ltd. 90-216-428-5933
- **Venezuela** InfoServices Consulting
Caracas 582-242-9141

Toll-Free Numbers

- **Sales and Partner Information** (866) 297-4929
- **VAR and Reseller Information** (212) 330-1710

Two Penn Plaza, New York, NY 10121-2898 (212) 330-1700 World Wide Web: www.iwaysoftware.com info@iwaysoftware.com

This product was produced in conjunction with XML Global, a leader in XML transformation, storage and search. www.xmlglobal.com 230 Park Avenue, Suite 1552, New York, NY 10169

Copyright © 2001 by iWay Software, Inc. All rights reserved. [54]

Java and all Java-based marks are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and other countries.

All products and product names mentioned in this publication are trademarks or registered trademarks of their respective companies.

DN3600573.0102