HIPAA Transactions: Testing and Certification

National HIPAA Summit Audioconference: Vendor And Clearinghouse Requirements For HIPAA Compliance

Larry Watkins
Vice President & COO, Claredi Corporation
Co-Chair, ASC X12N Health Care Task Group
Co-Chair, WEDI Strategic National Impl. Process (SNIP)
Breaking the cycle

• First phase: **testing**
  – Start testing as early as possible.
  – Confidential Testing against a neutral third party, not my trading partner.
  – Know where you are.

• Second phase: **certification**
  – Now I am really ready.
  – I want the world to know.
  – I can start engaging trading partners.

• Third Phase: **Business to Business**
  – Repeat for each “companion document” / TP
Testing today

- Find trading partner that agrees to test with you
  - Typically one that will eventually benefit from your transactions
- Send test files
- Get test report from trading partner
- Correct errors found by trading partner
- Repeat the cycle until no more errors
What the testing covers

- Telecommunications
- Security, authentication, access
- Data format issues
- Data content issues
  - Generic HIPAA requirements
  - Trading partner specific requirements
- Business rules
  - Some are HIPAA, some are trading partner specific requirements
Graphical view

- EDI Submitter contract
- Telecom / connectivity
- X12 syntax
- HIPAA syntax
- Situational requirements
- Code sets
- Balancing
- Line of business testing
- Trading partner specifics

- 1-2 days
- 2-3 weeks
- 1-2 days
- 3-4 weeks
The result of this testing

- Trading partner does not care about certain data elements
  - No errors reported this time
- Trading partner requires some data elements
  - Not an error for anybody else
- Is the error in the sender or the receiver of the transaction?
  - Cannot tell for sure.
  - Different interpretations.
Testing with multiple Trading Partners

TP Specific

Common in HIPAA
(2-3 weeks each)

TP Specific
The end result of today’s method of testing

- Repeat the testing for each trading partner.
- Common HIPAA requirements tested again from scratch each time.
- “Statistical Testing”
- Never sure of whether the testing is:
  - Complete, Correct, Repeatable.
- Very time consuming, expensive, wasteful, process.
- Unfair cost for the “readier” partner.
  - They end up debugging their trading partners.
The SNIP approach

• Compliance testing
  – Your own system, independent from trading partners
  – Structured testing; complete testing
  – HIPAA Implementation Guides

• Business to Business testing
  – Assume both trading partners are already compliant. Don’t repeat the compliance testing part
  – Test only peculiar TP issues
  – Companion Documents
SNIP Compliance testing

• “Types” of testing recommended by SNIP:
  1. EDI syntax integrity
  2. HIPAA syntactical requirements
     • Loops, valid segments, elements, codes
  3. Balancing of amounts
     • Claim, remittance, COB, etc.
  4. Situational requirements
     • Inter-segment dependencies
  5. External Code sets
     • X12, ICD-9, CPT4, HCPCS, Reason Codes, others
  6. Product Type, Specialty, or Line of Business
     • Oxygen, spinal manipulation, ambulance, anesthesia, DME, etc.
  7. Trading Partner Specific (NEW)
     • Medicare, Medicaid, Indian Health, in the HIPAA IGs.
Compliance testing

• Testing in both directions
  – Outgoing transactions
  – Incoming transactions

• Test for all SNIP test types ("levels")

• HIPAA Compliance
  – Specific requirements in the IGs

• Business requirements
  – Fuzzy general “industry knowledge”
  – Companion Documents
Testing with multiple Trading Partners

TP Specific

Common in HIPAA (2-3 weeks each)

TP Specific
Certification prior to Testing with multiple Trading Partners

TP Specific

Common in HIPAA (2-3 weeks total)

TP Specific
Certification prior to Testing with multiple Trading Partners

TP Specific

Common in HIPAA

TP Specific
The ideal HIPAA scenario

Trading Partner
Business to Business testing

Compliance testing
SNIP Compliance Testing

- Methodical vs. “statistical” (trial and error) testing process
- All types (levels) of test are required
  - Cannot stop at an arbitrary point
- Required compliance testing BEFORE starting the Business to Business testing process
- Recommends third party Certification of compliance
Compliance Certification

- Compliance Certification
- Compliance testing
- Trading Partner Business to Business testing
Certification vs. Testing

- Testing is for yourself (or between yourself and your trading partners as done today?)
- Certification is by third party
- Certify once, use certification in many trading partner relationships
  - Simplify testing, reduce to only companion document
  - Reduce cost of testing phase
- Certification should be recognized by all trading partners
- Certification must be done by a neutral third party
- Certification process must be disclosed, verifiable, and accepted by industry
Certification vs. Testing

- **Testing**
  - Private
  - For your own needs only
  - Test compliance
  - Test non-compliance
  - Never ending?
    User-defined

- **Certification**
  - Public statement
  - Also for other trading partners
  - Verify compliance
    - (Only positive assertion, no such thing as “certification of non-compliance”)
  - Well defined end point
Certification Challenge

• Each entity has unique requirements
  – Commercial business, HMO, Medicare
  – Generalist, specialist, ambulance, anesthesiologist, chiropractor, DME, etc.
• A “generic” certification is meaningless
• What does it mean to be “certified”?
• Must consider submitter capabilities and receiver requirements
The “clean test” myth

- If a transaction has no errors, it must be “HIPAA compliant”
Valid HIPAA Certification

• Certify your HIPAA compliance
  – Indicates capabilities related to requirement to comply with the HIPAA law
• Certify the transaction capabilities you have demonstrated to have. Both incoming and outgoing
  – Transaction capabilities as groups of data that represent the data needs of a business transaction
• Cannot certify your ability to send/receive invalid (syntax or HIPAA) transactions
• Cannot certify that all your outgoing transactions will always be compliant
The “vendor will fix it” myth

• My vendor / clearinghouse is HIPAA compliant. Why should I have to worry about it? They are going to take care of my HIPAA EDI compliance for me.
  – Providers and payers MUST get involved.
  – This is NOT an IT problem. It’s not Y2K
  – There are profound business implications in HIPAA.
The “Blanket Approval” myth
(Is testing of the vendor/clearinghouse enough?)

• The issue is Provider Compliance
  – Provider’s responsibility to be HIPAA compliant
• Each Provider is different
  – Different provider specialty ⇒ different requirements
  – Different software version ⇒ different data stream and contents
  – Different EDI format to clearinghouse ⇒ different content capabilities
  – Different provider site install ⇒ different customization
  – Different users ⇒ different use of code sets, different data captured, different practices, etc.
• Vendor’s capabilities not the same as provider’s
  – Vendor or clearinghouse has the aggregate capabilities of all its customers
  – The Provider does not have all of the clearinghouse or vendor capabilities
### Transaction Identifier

<table>
<thead>
<tr>
<th>Identifier</th>
<th>HIPAA Errors</th>
<th>Business Errors</th>
<th>Warnings</th>
</tr>
</thead>
<tbody>
<tr>
<td>PCLAM00001</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>PCLAM00002</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>154786686</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>234636898</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>476156866</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>432986866</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>435239866</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>534928666</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>

### Analysis Results to display

<table>
<thead>
<tr>
<th>WED/SNIP Levels</th>
<th>HIFAA Errors</th>
<th>Business Errors</th>
<th>Business Warnings</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 - X12 Integrity</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>2 - Requirement</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>3 - Balancing</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>4 - Situational</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>5 - Code Sets</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>6 - Product/Type</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Trading Partner</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

### Action

Display report:
- Errors and data
- Errors only
- Data only

Click here for the analysis report

### Certification

Please Review the Claredi Certification Policy

Status: Certification complete

### Support

You may allow Claredi Customer Support Reps to view the information in this file. Click here to review the Claredi Privacy Policy.
Certification Use for Clearinghouses

• Work with select clients to test and certify significant clearinghouse capabilities

• Use certification as gap analysis before moving clients into production
  – Test provider implementation
  – New specialties, converted formats, software versions, etc.

• Value Add – Match capabilities of providers with payers to ensure interoperability