

## **SOFTWARE APPLICATION ASSESSMENT**

To ensure that your organization will meet the transactional standards mandated by the HIPAA Standards for Electronic Transactions you should communicate with your software vendors to ensure that your software systems will be able to send insurance claims (and standard HIPAA transactions) in HIPAA-compliant formats.

This assessment gives vendors an opportunity to tell you what they've done so far and what they're planning regarding the new HIPAA standards. You can either submit the assessment to your vendor or speak to a technical person over the telephone to complete the questions.

## PART I: TRANSACTION STANDARDS

Below is a listing of the covered HIPAA transactions and the required HIPAA standards for each of them. Complete the requested information in the columns to the right of each standard.

HIPAA Covered Transaction	Transaction Standard	Currently Supported?	Will Be Supported?	Beta Release Date	Production Release Date
Health claims or equivalent encounter Information	Pharmacy—NCPDP Institutional—ASC X12N Health care claim (837) Professional—ASC X12N Health care claim (837) Dental—ADA Implementation guide for ASC X12N (837)				
Health care payment and remittance advice	<b>ASC X12N Health care claim—payment advice (835)</b>				
Health claim status	<b>ASC X12N Health care claim status request (276)</b> <b>ASC X12N Health care claim status notification (277)</b>				
Referral authorization	<b>ASC X12N Health care service review information (278)</b>				
Coordination of benefits	<b>Pharmacy—NCPDP Institutional—ASC X12N Health care claim (837)</b> <b>Professional—ASC X12N Health care claim (837)</b> <b>Dental—ADA Implementation guide for ASC X12N (837)</b>				
Health claims attachments*	<b>ASC X12N Patient information (275) with binary segment with HL7 content</b>				

This assessment questionnaire is used to evaluate software security features and should be completed in cooperation with the software vendor (if possible and where applicable)

Name of software, maker, version # \_\_\_\_\_

Question	Response
1. What is the authentication mechanism required with this application? <ul style="list-style-type: none"> <li>a. For the user?</li> <li>b. For administrators?</li> </ul>	
2. What security measures / parameters are used, e.g. — <ul style="list-style-type: none"> <li>a. User name?</li> <li>b. Minimum number of letters?</li> <li>c. Consists of name, letters, etc.?</li> <li>d. Who may change or add users?</li> </ul>	
3. Number of Administrators? <ul style="list-style-type: none"> <li>a. Who has authority to change or modify software parameters?</li> <li>b. Are there default passwords that came with the system?</li> <li>c. Have the default passwords been changed?</li> </ul>	
4. Does the system have an auto-logoff capability? <ul style="list-style-type: none"> <li>a. Is a password protected screen saver used?</li> </ul>	

Question	Response
5. Can the software limit access for a user to only certain parts of the system, dependent on job class or need of the individual?	
6. Is the software role-based? (How are access permissions given to use the system?)	
7. Does the application require / allow patient information to be sent over the Internet, modem or phone lines? a. Is information sent over the above channels encrypted?	
8. Can the users change their passwords whenever they wish?	
9. How many attempts can a user make at guessing his/her password before the system disconnects?	
10. Does the system disconnect users or revoke passwords?	
11. Do applications have separate logs or audit trail reports for events within the application?	
12. Are the actions of individual users recorded and used for accountability of their actions?	

Question	Response
<p>13. Can logs or audit trail records produce a chronological record of activity that allows reconstruction of transactions? Are modifications of files logged? Could the files be reconstructed?</p>	

To meet the HIPAA deadlines and maximize benefits from implementing HIPAA compliant solutions, your organization will need to invest wisely in new or upgraded healthcare information applications. HIPAA does not require your software vendor to comply, so software buyers and users must require them to comply or find an alternative software system.

Organizations will need to ask their existing or prospective vendors these questions:

1. Will there be an EDI solution?
  - a. If so, which of the standard HIPAA transactions will they support?
  
2. How will the vendor accommodate the new transactions and added data requirements?
  
3. Will the software vendor provide management solutions or tools to efficiently aid in converting to and using the new provider, employer, health plan and diagnostic and procedure code-sets?
  
4. How does the vendor plan to comply with the technical security safeguards?

[Software vendors will need to address mechanisms such as session time-outs, access controls and authorizations, backups and recovery, reporting of attempted intrusions, data integrity, possible encryption and eventually digital signatures.]