

HIPAA Snapshot Assessment Questionnaire

Prepared by

NAME OF CONSULTANT

Security		
I. Organizational Practices		
Inquiry		Response
1. Does your organization maintain a security/confidentiality committee?	All	
2. Who serves on the committee and what departments do they represent?	All	
3. How does the organization support and demonstrate implemented security measures?	All	
4. What is the policy on use of employee workstations?	All	
5. Does the organization provide security education and training programs for all employees, medical staff, agents and contractors?	All	
6. Are there organizational sanctions for violations of security policies and procedures?	All	
7. Does the organization maintain formal documentation of security plans, rules, procedures, and instructions concerning all components of the entity's security?	All	
8. Is there a security principle stating that a user should have access only to the data that he/she needs to perform a particular function?	All	

II. Personnel Controls		Response
Inquiry		
1. Have all positions been reviewed for sensitivity levels? If no, why?	H.R., Comp.	
2. Have employees filling those positions had the appropriate background investigations required? If no, why?	<i>H.R., Comp.</i>	
3. What are the employee termination procedures and are they documented?	All	
4. Are combination locks changed when employees are terminated?	All	
5. Are employees removed from access lists?	All	
6. Are user accounts deleted or deactivated?	All	
7. Are keys, tokens and cards, which allow access to secured areas revoked?	All	

III. Acquisition/Data/Network Controls		
Inquiry		Response
1. Does the organization maintain formal documentation of hardware and software assets?	I.S.	
2. Are there processes in place to prevent unauthorized manipulation of data and are unauthorized changes logged and reported when they occur?	All	
3. Are there policies and procedures in place to protect data transmitted across internal and external networks?	I.S.	
4. Are there policies and procedures to determine how health information will be disposed of securely, including destruction of media containing health information? What are they?	All	

V. Contingency Planning		
Inquiry		Response
1. Do you have a written disaster recovery plan in place that will take care of your critical operations? How often is this plan tested?	All	

VII. Security Awareness and Training		
Inquiry		Response
1. Are all users trained in the security policies of the organization?	All	
2. Are all managers trained in the security policies of the organization?	All	
3. What type of training is provided?	All	
4. How often are employees trained?	All	
5. Is automated information system security covered during new employee orientation?	All	
6. Are formal classes conducted periodically and specifically for the purpose of increasing the awareness of automated information systems security responsibilities?	All	
7. Are employees provided with posters, booklets, or other types of awareness material?	All	
8. Are seminars and workshops publicized and are employees encouraged to attend?	All	
9. Are the security P&P's documented? Do all users have access to this documentation?	All	
10. Are employees required to sign a statement regarding confidentiality of records?	All	
11. What are the defined escalation procedures, including contact names and numbers, for security issues?	All	

VIII. User Identification and Authentication		
Inquiry		Response
1. Do all users have individual passwords or are group passwords used on the system?	All	
2. Does a class of personnel exist within the organization that have been issued uniform/generic user ID's. If so which class and why?		
3. Is the password file protected by one-way encryption to prevent anyone (including the System Administrator) from reading the clear text passwords while stored on the system?	I.S.	
4. How many characters are required in your password by the core system you use? Is it an alphanumeric combination?	I.S.	
5. How often does the system (or System Administrator) force changing passwords?	I.S.	
6. How many generations have to pass prior to you being allowed to reuse a password you used before?	All	
7. Are users reminded to change their password when there is reason to believe it has been compromised?	I.S.	
8. How many attempts can a user make at guessing his/her password before the system disconnects?	All	
9. Does the system disconnect users or revoke ID/password?	All	

Section IX. Access Controls		Response
Inquiry		
1. Is access granted based upon Context, Role or User? (Context = transaction based)		
2. Are there controls in place to detect unauthorized transaction attempts either by authorized or unauthorized users?	All	
3. Are the actions of individual users recorded and used for accountability of their actions?	All	
A. Dial-In Access/Email/Fax:		
1. Can users dial into the system?	All	
2. Who has access through the dial-in lines?	I.S.	
3. Is protected health information ever sent via email unencrypted and unauthenticated?	All	
4. What type of data encryption is used?	I.S.	
5. What is the fax policy of this organization?	All	
B. Wide Area Networks:		
4. Is an alarm system in place for unauthorized use or access/intrusion of the network?	I.S.	
C. Data Integrity		
1. Is virus detection and elimination software used on the system?	All	

PRIVACY		
I. Uses and disclosure of protected health information		
Inquiry		Response
1. When is Subscriber/Members information disclosed?	All	
2. What measures taken to ensure that only the minimum amount of protected health information is disclosed to accomplish the intended purpose of the disclosure?	All	
3. Is protected health information ever disclosed over the phone? Under what circumstances?	All	
II. Notice to individuals of information practices		
Inquiry		Response
1. Does a Subscriber/Members receive notice of the policies and procedures with respect to protected health information?	M.R., Comp.	
2. Is notice to individuals provided regarding their rights and the procedures for exercising their rights?	All	

III. Subscriber/Members rights		
Inquiry		Response
1. Does an individual have the right to request the following with respect to his or her protected health information: <ul style="list-style-type: none"> • Inspection and copying • Amendment or correction • An account of the disclosures of such information by the organization 	M.R., Comp.	
IV. Administrative requirements		
Inquiry		Response
1. Is there a designated privacy officer or committee? Do duties include development and implementation of privacy policies and procedures?	All	
2. Is there a contact person or office responsible for receiving complaints and providing further information about protected health information matters?	All	
3. Is there a hot line for employees to call to file complaints or report infractions?	All	
4. Who is responsible for investigating complaints and infractions?	All	
5. How is the individual notified of the results of the investigation?	All	
6. What types of privacy training are available to the workforce?	All	
7. What are the policies for whistleblowers?	All	
8. What are the sanctions for failing to comply with privacy policies and procedures?	All	

INDIVIDUALLY IDENTIFIABLE HEALTH INFORMATION

- (A) Names;
- (B) Postal address information, other than town or city, State,
and zip code;
- (C) Telephone numbers;
- (D) Fax numbers;
- (E) Electronic mail addresses;
- (F) Social security numbers;
- (G) Medical record numbers;
- (H) Health plan beneficiary numbers;
- (I) Account numbers;
- (J) Certificate/license numbers;
- (K) Vehicle identifiers and serial numbers, including license plate numbers;
- (L) Device identifiers and serial numbers;
- (M) Web Universal Resource Locators (URLs);
- (N) Internet Protocol (IP) address numbers;
- (O) Biometric identifiers, including finger and voice prints;
- (P) Full face photographic images and any comparable images

HHS Business Partner Assessment Summary

This document is designed to identify all HIPAA classified business partners within a given covered entity. Covered entities may disclose protected health information (“PHI”) to a business associate and may allow the business associate to create or receive information on its behalf. The covered entity must obtain “satisfactory assurance” that the business associate will safeguard the protected health information. This “satisfactory assurance” must be documented through a written contract or agreement.

Sample HIPAA Business Partner Assessment Summary

<i>Partner Name and Type (Trading Partner or Business Associate)</i>	<i>Product/Service</i>	<i>Communication & Coordination Structure?</i>	<i>Compliance Dates Established?</i>	<i>Contract in Place? HIPAA provisions?</i>	<i>Comments</i>
Network (Trading Partner)	Clearinghouse	No. Client sent request to establish contacts and implementation coordination process	No. Need specific details regarding testing, migration, and final implementation dates	Yes. However, contract needs updates to reflect required security and privacy provisions	
Software Company (Business Associate)	Hospital Information System	Yes.	No. Current vendor commitment does not specify testing and release dates	Yes. However provisions needed to meet Business Associate requirements	
<i>Summary</i>					
<i>Total number business partners</i>		<i>% Completed</i>	<i>% Completed</i>	<i>% Completed</i>	
2		50%	0%	0%	