ABC Company

InhouseCIO

The IT Department for Small Business

HIPAA Questionnaire & Site Survey

ABC Company

Prepared by:

InhouseCIO, LLC

Date:

Contents

Pre-assessment Documentation

Prior to performing the assessment, you should protect yourself by signing a HIPAA Business Associate Agreement.

Topic	Instructions/Notes	Choices	Exclude?
Business Associate Agreement	***Do you have a signed Business Associate Agreement with the party that will be conducting the assessment? If 'no', do not proceed with the assessment.***	☐ *Yes* ☐ *No* ☐ *N/A*	

Security Officer

HIPAA requires a named Security Officer as a central point of contact. Enter information for the Security Officer in this section.

Topic	Instructions/Notes	Responded By	Exclude?
Name	***Enter the name of the Security Officer for the practice***		
Contact Information	***Enter contact information for the Security Officer. You can use multiple lines if needed.***		

Physical Access Security Measures

HIPAA requires that physical access controls—doors, locks, cabinets, cages, locking cables, and employee training—be implemented to protect health information.

Topic	Instructions/Notes	Choices	Exclude?
Access Control Procedure	***Does the practice have a written policy and procedure for granting access to ePHI? Include a copy of the policy and procedure with the assessment.***	☐ *Yes* ☐ *No*	
Employee Training	***Do all employees receive training on how to avoid becoming a victim of technology threats? Please validate records of the training for all employees are available before answering Yes.***	☐ *Yes* ☐ *No*	
Biometric or Multi-Factor Authentication	***Does the practice use biometric authentication, security cards, or codes for logon?***	☐ *All* ☐ *Some* ☐ *None*	

Data Center

A data center is any third-party organization that hosts ePHI on servers or storage devices, no matter if owned by the client, a cloud service provider, or the data center. The HIPAA Omnibus Final Rule (2013) requires data centers to comply as HIPAA Business Associates because they 'maintain' data even if it is encrypted, or they cannot or do not access the data.

Topic	Instructions/Notes	Choices	Exclude?
Hosted Servers	***Does the practice have servers that could have or could possibly transmit ePHI in a hosted facility or external data center?***	☐ *Yes* ☐ *No*	
Business Associate Agreement	***If yes to the above, do you have a Business Associate Agreement with the Data Center?***	☐ *Yes* ☐ *No* ☐ *N/A*	

External Firewall

An External Firewall is a device used to protect a network from external attacks. Firewall functionality may be built into some routers. In those cases, the router models should be investigated for additional functionality. Firewalls include Intrusion Detection and Intrusion Prevention features. Many also offer network perimeter protection against viruses and other malware.

Topic	Instructions/Notes	Choices	Exclude?
External Firewall	***Does your practice employ an external firewall to protect your network from external attacks? Please list the model numbers of all firewalls in use in the Notes area (one per line).***	☐ *Yes* ☐ *No*	
Intrusion Prevention System	***Does the firewall have an Intrusion Prevention System (IPS)?***	☐ *Yes* ☐ *No* ☐ *Don't know* ☐ *N/A*	
Intrusion Prevention System Turned On	***Is the Intrusion Prevention system (IPS) turned on?***	☐ *Yes* ☐ *No* ☐ *Don't know* ☐ *N/A*	
Malware Filtering	***Does the external firewall have Malware Filtering?***	☐ *Yes* ☐ *No* ☐ *Don't know* ☐ *N/A*	

Malware Filtering Subscription Current	***Is Malware Filtering current?***	☐ *Yes* ☐ *No* ☐ *Don't know* ☐ *N/A*	

Office Walkthrough

Seeing is believing. Everything from the layout of the office, locks and other methods to secure devices, and how visitors are managed should be observed.

Topic	Instructions/Notes	Choices	Exclude?
Physical Computers Security	***During a physical walkthrough of the office, were any computers not secured against theft? Methods can include physical security cabling, door locks, electronic access control systems, security officers, or video monitoring. Enter findings in the Notes area if you select Yes.***	☐ *Yes* ☐ *No*	
Data Storage Devices Security	***During a physical walkthrough of the office, were any data storage devices not secured against theft? Methods can include locked cabinets, door locks, electronic access control systems, security officers or video monitoring. Enter findings in the Notes area if you select Yes.***	☐ *Yes* ☐ *No*	
Viewable Screens by Co-Workers or Visitors	***Are there any workstation screens that potentially have ePHI viewable by the public or co-workers (answer 'no' if only a user seated behind the screen can view it)? Enter findings in the Notes area if you selected Yes.***	☐ *Yes* ☐ *No*	
Retired/Decommissioned/Failed Systems or Storage Devices	***Are there any retired, decommissioned, failed systems or storage devices present? Enter findings in the Notes area if you select Yes.***	☐ *Yes* ☐ *No*	
Copiers and Multi-function Printers	***Does your company use any copiers or multi-function printers? Please list all model numbers below.***	☐ *Yes* ☐ *No*	

Wireless

Wireless networks are often overlooked as a security vulnerability. While a hacker or former employee may not be able to enter a facility to plug into a network, they may be able to park outside or come close enough to get wireless access.

Topic	Instructions/Notes	Choices	Exclude?
Guest Wireless	***Does your company provide guest wireless to visitors or patients?***	☐ *Yes* ☐ *No*	
Guest Wireless Same Network as ePHI	***Is your guest wireless access on the same network as ePHI? Such as on the same network as doctors and nurses. If you do not have guest wireless, answer 'N/A'.***	☐ *Yes* ☐ *No* ☐ *N/A*	

Topic	Instructions/Notes	Responded By	Exclude?
Days since Wireless Key Changed	***Enter the number of days since the wireless key was last changed below.***		
High Risk Users Terminations since Last Wireless Key Change	***High Users Employees should include anyone with administrative access, such as an IT person. Enter 'yes' if there have been high risk employee or vendor terminations since the last wireless key change in the notes. If not, then enter 'no'***		
Wireless SSID	***List all published SSID (one per line).***		

Fax

Faxing used to be paper documents being sent and paper documents received. Today faxes can be originated or received electronically, with images stored locally or with vendors.

Topic	Instructions/Notes	Choices	Exclude?
How do you send FAX?		☐ *Paper* ☐ *Electronic Fax Local* ☐ *Electronic Fax Service* ☐ *Paper and Electronic Fax Local* ☐ *Paper and Electronic Fax Service* ☐ *N/A*	
Business Associate Agreement	***If Electronic Fax Service above, do you have a Business Associate Agreement with the Electronic Fax Service?***	☐ *Yes* ☐ *No* ☐ *N/A*	
How do you receive FAX?		☐ *Paper* ☐ *Electronic Fax Local* ☐ *Electronic Fax Service* ☐ *Paper and Electronic Fax Local* ☐ *Paper and Electronic Fax Service* ☐ *N/A*	

Business Associate Agreement	***If Electronic Fax Service above, do you have a Business Associate Agreement with the Electronic Fax Service? If you do not have service, answer 'N/A'.***	☐ *Yes* ☐ *No* ☐ *N/A*	

Email

E-mail is a common tool used for business and personal communications. ePHI should only be sent within, or attached to, an e-mail message within a secure network or if the service complies with HIPAA and has signed a Business Associate Agreement.

Topic	Instructions/Notes	Choices	Exclude?
Use Free Email Service	***Do your employees ever send email containing PHI to free email accounts, including Gmail, Hotmail, Yahoo, or free accounts from Internet Service Providers? List the providers in the Notes area one per line.***	☐ *Yes* ☐ *No*	
Business Associate Agreement	***If yes to the above, do you have a Business Associate Agreement with all the above free providers?***	☐ *Yes* ☐ *No* ☐ *N/A*	

Electronic Health Record System

Topic	Instructions/Notes	Choices	Exclude?
Local EHR Server	***Does your practice use a local EHR system (not cloud-based)?***	☐ *Yes* ☐ *No*	
Is EHR Server secured?	***Is the server in a locked room, locked cabinet, or locked down? If no, please enter the reason you do not feel that your server does not need to be secured below.***	☐ *Yes* ☐ *No*	
Cloud-based EHR System	***Does your company use a cloud-based EHR system? Enter the name of the cloud-based provider in the Notes field.***	☐ *Yes* ☐ *No*	
Business Associate Agreement	***If yes to the above, do you have a Business Associate Agreement with your EHR vendor?***	☐ *Yes* ☐ *No*	