YourIT!
Your Logo Goes Here

HIPAA Assessment

HIPAA On-Site Survey

Scan Date: 12/13/2018

Prepared for:
HIPAA – Covered Entity
Prepared by:
YourIT Company

12/16/2018

Table of Contents

Security Officer

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

Name

Enter the name of the Security Officer for the covered entity.

Response Bob Smith	**Responded By**
Additional Notes	

Contact Information

Enter contact information for the Security Officer. You can use multiple lines if needed.

Response 555-555-5555 bobsmith@hipaa-covered-entity.com	**Responded By**
Additional Notes	

Pre-assessment Documentation

Prior to performing the assessment you should protect yourself and your client by signing a HIPAA Business Associate Agreement and having your client sign a letter authorizing the assessment including the external vulnerability test.

Business Associate Agreement

If you are a 3rd party performing this assessment, do you have a signed Business Associate Agreement? If 'no', do not proceed with the assessment.

Response	**Responded By**
Yes	
Additional Notes	

Signed Authorization

If you are a 3rd party performing this assessment, do you have a signed authorization to perform the assessment? If 'no', do not proceed with the assessment.

Response	**Responded By**
Yes	
Additional Notes	

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.

Access Control Procedure

Does the company have a written policy and procedure for granting access to ePHI? Include a copy of the policy and procedure with the assessment.

Response	**Responded By**
No	
Additional Notes	

Employee Training

Do all company 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.

Response	**Responded By**
No	
Additional Notes	

Biometric or Multi-Factor Authentication

Does your company use biometric authentication, security cards, or codes for logon?

Response	**Responded By**
Some	
Additional Notes	

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.

Hosted Servers

Does your company have servers that could have or could possibly transmit ePHI in a hosted facility or external data center?

Response	**Responded By**
Yes	
Additional Notes	

Follow-up to if you answered Yes above
Business Associate Agreement

If yes to the above, do you have a Business Associate Agreement with the Data Center?

Response	**Responded By**
No	
Additional Notes	

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.

External Firewall

Does your company 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).

Response	**Responded By**
Yes	
Additional Notes	

Follow-up to if you answered Yes above
Intrusion Prevention System

Does the firewall have an Intrusion Prevention System (IPS)?

Response	**Responded By**
No	
Additional Notes	

Follow-up to if you answered Yes above
Malware Filtering

Does the external firewall have Malware Filtering?

Response	**Responded By**
No	
Additional Notes	

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.

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.

Response	**Responded By**
Yes	
Additional Notes	

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.

Response	**Responded By**
Yes	
Additional Notes	

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.

Response	**Responded By**
Yes	
Additional Notes	

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.

Response	**Responded By**
Yes	
Additional Notes	

Copiers and Multi-function Printers

Does your company use any copiers or multi-function printers? Please list all model numbers below.

Response	Responded By
No	
Additional Notes	

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.

Guest Wireless

Does your company provide guest wireless to visitors or patients?

Response	**Responded By**
Yes	
Additional Notes	

Follow-up to if you answered Yes above
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'.

Response	**Responded By**
N/A	
Additional Notes	

Office Wireless

Does your company provide wireless to employees or vendors?

Response	**Responded By**
No	
Additional Notes	

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.

How do you send FAX?

Response Paper and Electronic Fax Service	**Responded By**
Additional Notes	

Follow-up to if you answered Paper and Electronic Fax Service above
Business Associate Agreement

If Electronic Fax Service above, do you have a Business Associate Agreement with the Electronic Fax Service?

Response No	**Responded By**
Additional Notes	

How do you receive FAX?

Response Paper and Electronic Fax Service	**Responded By**
Additional Notes	

Follow-up to if you answered Paper and Electronic Fax Service above
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'.

Response N/A	**Responded By**
Additional Notes	

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.

Use Free Email Service

Do your employees ever send or receive email containing PHI from free email accounts, including Gmail, Hotmail, Yahoo, or free accounts from Internet Service Providers? List the providers in the Notes area one per line.

Response	**Responded By**
Yes	

Additional Notes
gmail google

Follow-up to if you answered Yes above
Business Associate Agreement

If yes to the above, do you have a Business Associate Agreement with all the above free providers?

Response	**Responded By**
No	

Additional Notes

Electronic Health Record System

Local EHR Server

Does your company use a local EHR system (not cloud-based)?

Response Yes	**Responded By**
Additional Notes	

Follow-up to if you answered Yes above
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.

Response Yes	**Responded By**
Additional Notes	

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.

Response No	**Responded By**
Additional Notes	