



# HIPAA Assessment

## Response Report - HIPAA On-Site Survey



**CONFIDENTIALITY NOTE:** The information contained in this report document is for the exclusive use of the client specified above and may contain confidential, privileged and non-disclosable information. If the recipient of this report is not the client or addressee, such recipient is strictly prohibited from reading, photocopying, distributing or otherwise using this report or its contents in any way.

Prepared for:  
Customer Name Here!  
Prepared by:  
YourIT! Company, Inc.

## Table of Contents

- 1 - Pre-assessment Documentation
- 2 - Physical Access Security Measures
- 3 - Data Center
- 4 - External Firewall
- 5 - Office Walkthrough
- 6 - Wireless
- 7 - Fax
- 8 - Email
- 9 - Electronic Health Record System

## 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.*

Topic	Notes	Response
Business Associate Agreement		<input checked="" type="checkbox"/> Yes
Signed Authorization		<input checked="" type="checkbox"/> Yes

## 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	Notes	Response
Access Control Procedure		<input checked="" type="checkbox"/> Yes
Employee Training		<input checked="" type="checkbox"/> No
Biometric or Multi-Factor Authentication		<input checked="" type="checkbox"/> 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	Notes	Response
Hosted Servers		<input checked="" type="checkbox"/> Yes
Business Associate Agreement		<input checked="" type="checkbox"/> No

## 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	Notes	Response
External Firewall	ASA-5100	<input checked="" type="checkbox"/> Yes
Intrusion Prevention System		<input checked="" type="checkbox"/> Yes
Intrusion Prevention System Turned On		<input checked="" type="checkbox"/> No
Malware Filtering		<input checked="" type="checkbox"/> Don't know
Malware Filtering Subscription Current		<input checked="" type="checkbox"/> Don't know

## 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	Notes	Response
Physical Computers Security	Defunct computers and drives left on desks.	<input checked="" type="checkbox"/> No
Data Storage Devices Security	USB drives in common area.	<input checked="" type="checkbox"/> Yes
Viewable Screens by Co-Workers or Visitors		<input checked="" type="checkbox"/> No
Retired/Decommissioned/Failed Systems or Storage Devices	Computers stored under desk in reception.	<input checked="" type="checkbox"/> Yes
Copiers and Multi-function Printers	Canon 4432 A	<input checked="" type="checkbox"/> Yes

## 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	Notes	Response
Guest Wireless		<input checked="" type="checkbox"/> Yes
Guest Wireless Same Network as ePHI		<input checked="" type="checkbox"/> Yes



## 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	Notes	Response
How do you send FAX?		<input checked="" type="checkbox"/> Paper and Electronic Fax Service
Business Associate Agreement		<input checked="" type="checkbox"/> No
How do you receive FAX?		<input checked="" type="checkbox"/> Paper and Electronic Fax Service
Business Associate Agreement		<input checked="" type="checkbox"/> No

## 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	Notes	Response
Use Free Email Service	Gmail	<input checked="" type="checkbox"/> Yes
Business Associate Agreement		<input checked="" type="checkbox"/> No

## Electronic Health Record System

Topic	Notes	Response
Local EHR Server		<input checked="" type="checkbox"/> <i>No</i>
Is EHR Server secured?		<input checked="" type="checkbox"/> <i>Yes</i>
Cloud-based EHR System		<input checked="" type="checkbox"/> <i>No</i>
Business Associate Agreement		<input checked="" type="checkbox"/> <i>No</i>