

**HIPAA**

**Assessment**

Evidence of HIPAA Policy Compliance



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 by:

ICore Pioneer Business solutions. Prepared for: Ancel Medical Transcription 25/04/2018

# Table of Contents

1. - [Overview](#_bookmark0)
2. - [Overall Risk](#_bookmark1)

2.1 - [Conduct Risk Assessment](#_bookmark2) 3 - [Environment](#_bookmark3)

3.1 - [Facility Access Controls](#_bookmark4) 4 - [Users](#_bookmark5)

* 1. - [Information System Activity Review / Unique User Identification](#_bookmark6)
  2. - [Establish Clear Job Description and Responsibilities / Access Authorization](#_bookmark8)
  3. - [Evaluate Existing Security Measures Related to Access Controls](#_bookmark9)
  4. - [Password Management](#_bookmark10)
  5. - [Administrative Access Control](#_bookmark11)
  6. - [Audit Controls](#_bookmark12)
  7. - [Person or Entity Authentication](#_bookmark13) 5 - [Servers and Local Computers](#_bookmark14)
  8. - [Protection Against Malicious Software](#_bookmark15)
  9. - [Applications and Data Criticality Analysis](#_bookmark16)
  10. - [Business Associate Agreements for Cloud Servers and Data Centers](#_bookmark17)
      1. - [Data Center](#_bookmark18)
      2. - eFax Service
      3. - [Remote Access Cloud Services](#_bookmark19)

5.5 - Business Associate Agreements for Sync folders (DropBox, Box, Google Drive, etc. ) 6 - [Firewall](#_bookmark20)

* 1. - [Access Authorization](#_bookmark21)
  2. - [Protection Against Malicious Software](#_bookmark22)
  3. - [External Vulnerability Scan Analysis](#_bookmark23) 7 - [Email](#_bookmark24)

7.1 - [Applications and Data Criticality Analysis](#_bookmark25) 8 - [Wireless](#_bookmark26)

* 1. - [Access Authorization](#_bookmark27)
  2. - [Access Establishment](#_bookmark28)
  3. - [Workforce Security](#_bookmark29)

# 1 - Overview

Our organization has adopted written Policies & Procedures that describe in detail the tasks that we have committed to undertake to fulfill our HIPAA compliance reporting requirements.

We start by performing a periodic Risk Analysis to identify threats and vulnerabilities to ePHI and the security of our networks and systems, in general. We then create a Risk Management Plan to prioritize remediation and ensure resolution of the issues identified in the Risk Analysis.

This document supplements the Risk Analysis and Risk Management Plan and offers substantiation and verification of policy compliance by providing confirmation of timely performance of recommendations detailed in the Risk Management Plan.

**Security Officer**

*Name of Security Officer:* Krishna Kumar

# - Overall Risk

**2.1 - Overall Risk**

We have performed a Risk Assessment as part of our routine HIPAA compliance review.

The Risk Analysis is designed to accurately and thoroughly identify vulnerabilities and threats that impact electronic Protected Health Information (ePHI). The report is then used to assess the potential risks to the confidentiality, integrity and availability of ePHI located or held at our office.

The Risk Analysis follows industry best practice standards as described by HHS, NIST, ISACA, HIMSS or AHIMA organizations and performed no less than one time a year or after successful implementation of any major system change including an office relocation, replacement of EHR system containing PHI, etc.

# - Environment

**3.1 - Facility Access Controls**

1. Here implement procedures that are designed to allow authorized access and deny unauthorized access, to and within facilities, to limit access to devices that can access.
2. Electronic devices like mobile banned at production floor

## Computers

During a physical walkthrough, we found

1. Computers that have protection against Read/Write removable storage access like Pen drive, External HDD.
2. Here have a physical server; employees can access individual system through as domain user.
3. Restricted internet access; users only can access Google, almost all social media site has banned.
4. User’s computer protected using firewall and antivirus software

# - Users

**4.1 - Information System Activity Review / Unique User Identification**

1. Here employ the use of Windows Authenticated users as a means for unique user identification.
2. As part our regular review of system activity, we validate the list of current users and identify former employees and vendors who may still have access. This review involves looking at audit logs, access reports, and reviewing security incident tracking reports. During the review, generic accounts logins are also identified for further investigation.
3. A signed legal NDA with employee

**4.1 - Password Management**

Proper password management is vital for ensuring the security of the network. Password complexity and expiration policy should be enabled and enforced by Group Policy when possible.

|  |  |  |
| --- | --- | --- |
| Policy | Setting | Computers |
| Enforce password history | 0 passwords remembered | All Sampled |
| Maximum password age | 42 days | All Sampled |
| Minimum password age | 1 days | All Sampled |
| Minimum password length | 7 characters | All Sampled |
| Password must meet complexity requirements | Enabled | All Sampled |
| Store passwords using reversible encryption | Disabled | All Sampled |

Proper account lockout policy settings will prevent both interactive and automated attempts to compromise passwords.

Comment: Except for service accounts, all passwords for users that can potentially log in should be set to expire on a regular basis.

**4.2 - Administrative Access Control**

Automatic log off or lockout is to be set on all computers. Lockout time should always be less than 5 minutes.

|  |  |
| --- | --- |
| Lockout Time (minutes) | # Computers |
| <=5 | All Sampled |

1. **- Servers and Local Computers**

**5.1 - Protection Against Malicious Software**

**Endpoint Security Summary**

This section contains a listing of detected Antivirus, Antispyware, Firewall, and Backup information as detected through *Security Center* and/or *Installed Services* for major vendors, which is then categorized by domain membership.

Values in the "Name" column contain either the name of the product, None indicating the machine returned information but no product was found, or <empty> indicating information was not obtainable. Further, a status of ****indicates "yes", ****indicates "no", and <empty> indicates that a status was not available.

# - Firewall

**6.1 - Access Authorization**

### We employ an external firewall to prevent external attacks.

**6.2 - Protection Against Malicious Software**

### The external firewall does not have Malware Filtering. The firewall may not be a commercial grade firewall and should be upgraded.

**6.3 - External Vulnerability Scan**

As part of our routine procedure to ensure protection from external threats, we have conducted an external vulnerability scan. The following external IP addresses were scanned and accessed:

# - Wireless

**7.1 - Access Authorization**

The following wireless access points were detected. Highlighted entries are SSID published by our company. We discourage the use of all non-company wireless access points.

|  |  |  |  |
| --- | --- | --- | --- |
| SSID | Secured | Security | Risk Level |
| *No wireless networks detected* | | | |

**7.2 - Access Establishment**

The wireless keys were last changed **25 days ago**.

**7.3 - Workforce Security**

The wireless key has been changed since the latest high risk employee termination.