iCore Pioneer
Business Solution

Evidence of Security Assessment

Prepared by : ICore Pioneer Business Solution Pvt Ltd.
Prepared for : Ansell Medical Transcription
Dated : 25th April 2018

Table of Contents

1 - Overview

Based on the discussion with Ansell Medical Transcription Company, iCore Pioneer Business Solution Pvt Ltd. did a security assessment at their Trivandrum and Ernakulum offices on 25th April 2018. Our staff visited both offices and had a detailed discussion with the System Administrator(s) associated; and also physically evaluated their overall facility, infrastructure, security practices etc. As there was not much lead time given for the assessment, iCore did perform an overall checking, collected sample data, and did some random inspection only. But we recommend conducting this kind of assessment on a half yearly/yearly basis and ensuring the compliance of company operations.

After such assessments, kindly ensure that the observations/suggestions are getting implemented and closed on a timely basis to avoid any vulnerability incident(s)/breaches in future.

We did perform an overall Risk Analysis to identify threats and vulnerabilities, the security of networks and systems, in general. Based on the preliminary random assessment, we have few observations and documenting the same in below sections.

Security Officer

Name of Security Officer: Sameer M J

2- Overall Observations

2.1 - Overall Observations

We have performed a Risk Assessment as part of our information security 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 your office(s).

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.

3- Environment

3.1 - Facility Access Controls

1. Work place protected with access control system. The facility is designed to allow authorized access and deny unauthorized access.
2. Electronic devices like mobile phones are banned at production floor

Computers

During a physical walkthrough, we found

1. Computers are protected against Read/Write removable storage access like Pen drive, External HDD etc.
2. The existing physical server; employees can access individual system through domain user only.
3. Restricted internet access: Based on the discussion with managers, we realized that the users only can access Google. While doing a random checking, we observed almost all social media sites are banned at work PC's. (Only few PC's tested due to lack of time.)
4. Servers protected using firewall and antivirus software and the softwares are updated as well.

File Access

1. Presently the employees can access/copy audio files as well as documents. Even they can send it to personal ID's. We recommend a control point by restricting this by the implementation of software so that the files can only access via software.

4- Users

4.1 - Information System Activity Review / Unique User Identification

1. Here employ uses 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. During the review, generic accounts logins are also identified for further investigation.
3. During the interaction with different levels of employees, we observed that every individual employee is obliged to sign a legal NDA with company. Randomly checked few of them as well.

4.2 - Password Management

Based on the interaction with managers, we believe proper password management followed in the companies for ensuring the security of the network. Password complexity and expiration policy should be enabled and enforced by Group Policy when possible.

Comment:

- Except for service accounts, all passwords for users that can potentially log in should be set to expire on a regular basis.
- Recommending a detailed review on Enforce password history, Maximum & Minimum password age, password length, Password complexity etc. in policy/settings in all the computers rather than doing a sampling during next time.
- Proper account lockout policy settings will prevent both interactive and automated attempts to compromise passwords.

4.3 - 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

5- Firewall

5.1 - 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- Email

6.1-Applications and Data Criticality Analysis

Users can send emails to outside world. There is a potential threat that the users can send the patient information to outside world via email. We recommend a control point via the medical transcription software to prevent storing the patient data in local PC rather the access of data is only via the software.