Revision	Author/Reviewer	Comments	Date created/modified
4	Danny Lieberman	Security audit report to Neurotech Solutions	11/03/2012

HIPAA Security Assessment – Neurotech Solutions Ltd.

Executive summmary

The following security assessment addressess the Neurotech implementation of the HIPAA Security Rule technical, administrative and physical safeguards according to Appendix A Subpart C of Part 164, of HIPAA Security Standards.

The security assessment relates to a situation where Neurotech is a vendor acting as a “business associate” to a HIPAA "covered entity". As stated in CFR 45 §164.314 (2) (i):

> “*The contract between a covered entity and a business associate must provide that the business associate will implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the covered entity”.*

Although Neurotech is neither a covered entity nor a health care clearinghouse under the administrative simplification provisions of HIPAA (CFR 45[1]), the company is commited to patient privacy and has implemented the appropriate technical, administrative and physical security safeguards in order to minimize the risk of unauthorized disclosure of ePHI (electronic protected health information) at customers who use their products and services. The company Information Security policy (see company document **Neurotech_SecurityPolicy**) sets standards for information security management, planning, execution and monitoring.

Danny Lieberman

D. Lieberman

Managing Partner
Software Associates – security and compliance specialists for medical device and healthcare companies

[1] http://www.hhs.gov/ocr/privacy/hipaa/administrative/combined/index.html

Introduction

A security audit of the Neurotech (“the company”) MOXO ADHD Test was performed in January - February 2012. The security audit included interviews with Neurotech engineering and operations staff including a white-box penetration test of the Web application in order to simulate actions of a malicious insider who has knowledge of and credentials to access the target system.

The output of the audit is the following report. The results are organized and numbered according to the security safeguards specified in Appendix A Subpart C of Part 164, of HIPAA Security Standards. Legal and regulatory guidance regarding HHS and FDA rules are outside the scope of the assessment.

The security safeguards are grouped into 2 color-coded groups:

- Group I – End-user customer responsibility
- Group II – Company responsibility

HIPAA Audit report

Notes: A – Addressable safeguards, R – Required safeguards

164.308 Administrative safeguards

(1) Security management process

A) **Risk Analysis (R)**: As part of the risk management process, the company performs information security risk analysis for its services (see company procedure **Neurotech_RAM.1**) analyzing software security, data security and human related vulnerabilities. Risk analysis is performed according to the Practical Threat Analysis methodology.

B) **Risk Management (R)**: Company procedure Neurotech_RAM.1 defines the methodology by which the risks of information security threats are systematically identified and evaluated and to ensure that adequate actions are taken to reduce risk to acceptable levels.

C) **Sanction Policy (R)**: HIPAA requires that covered entities have and apply appropriate sanctions against members of their workforce who fail to comply with Privacy Policies and Procedures of the entity, or the requirements of the Rule (45 CFR SS 164.530(e)(1)

D) **Information System Activity Review (R)**: The company has implemented a systematic system activity review process using the Practical Threat Analysis methodology and conducts a yearly activity review, in order to assess the current security risk profile of the product.

(2) Assigned security responsibility (R)

The CTO, Mr. Kinor has been assigned security responsibility and is co-lead of the IRT (incident response team).

(3) Workforce security

A) Authorization and/or Supervision (A)
B) Workforce Clearance Procedure
C) Termination Procedures (A)

Note: The company enforces Acceptable Usage and Data Governance policies for it's own employees. See company procedures **Neurotech_AUP** and **Neurotech_DGP**.

(4) Information access management

A) Isolating Health care Clearinghouse Function (R)
B) Access Authorization (A)

C) Access Establishment and Modification (A)

Note: The company requires a signed NDA from all employees and contractors in order to protect Confidential information including customer data.

(5) Security awareness and training

A) Security Reminders (A)
B) Protection from Malicious Software (A)
C) Log-in Monitoring (A)
D) Password Management (A)

Note: The company performs security awareness training is performed once/year for its own employees. The company enforces Acceptable Usage and Data Governance policies for it's own employees. See procedures **Neurotech_AUP** and **Neurotech_DGP**.

(6) Security incident procedures

Response and Reporting (R)

See the company procedure **Neurotech_IRP.1** that describes the process used by Neurotech to manage information security incidents and internal or external attacks on confidentiality, integrity or availability of company assets.

(7) Contingency plan

A) Data Backup Plan (R)
B) Disaster Recovery Plan (R)
C) Emergency Mode Operation Plan (R)
D) Testing and Revision Procedure (A)
E) Applications and Data Criticality Analysis (A)

See the attached compay procedure **Neurotech_DRP.1** that describes the planning and implementation process for disaster recovery for the Neurotech office and Web application operations.

(8) Evaluation(R)

The company evaluates it's security policies on an annual basis as part of the Security Management Process. See company procedure **Neurotech_RAM.1** that describes the structured process used by Neurotech for risk analysis and ongoing risk management.

(9) Business associated contracts

Written Contract or Other Arrangement (R)

Company contractors and employees that interface with end user customers have signed the company NDA

164.310 Physical safeguards

(1) Facility access controls

A) Contingency Operations (A)
B) Facility Security Plan (A)
C) Access Control and Validation Procedures (A)
D) Maintenance Records (A)

Note: The company uses SAS-70 compliant services from Rackspace for its managed cloud instances.

In the course of ongoing product support, company employees may come in contact with PHI at customer request. Company security policy is not to store any PHI in company offices and not to retain any ePHI on magnetic media or paper records.

(2) Workstation use (R)

Appropriate use of personal computer workstations is subject to the end-user customer Appropriate Usage Policy. The MOXO ADHD test terms of service clearly stipulate that IT and end-point security is the sole responsibility of the customer.

Note: The company enforces Acceptable Usage and Data Governance policies for it's own employees. See procedures **Neurotech_AUP** and **Neurotech_DGP**

(3) Workstation, notebooks and servers security (R)

Windows and Linux workstations in company premises
The company supports standard system configurations for Windows 7/SP2 and Ubuntu 11.10.

Access by company employees and contractors
Company employees and contractors use Windows 7 based workstations and a standard Firefox or Google Chrome browser in order to provide customer support.

Office workstations and notebooks used by company employees and field service technicians use Microsoft Windows 7 SP 2 and have the latest McAfee anti-virus from with ongoing software updates of the OS and anti-virus software.

(4) Device and media controls including USB flash drives that may be used as an attack vector for ePHI disclosure

A) Disposal (R), Media Re-use (R)
B) Accountability (A)
C) Data Backup and Storage (A)

Note: The company enforces Acceptable Usage and Data Governance policies for it's own employees. See procedures **Neurotech_AUP** and **Neurotech_DGP**

164.212 Technical safeguards

(1) Access control

A) Unique User Identification (R) -
1. **Application user login credentials:** Unique application user identification is provided via the admin create user function or admin edit user function after a user has registered online. Application user passwords are stored using a one-way hash in a PostgreSQL 9.1 database server.
2. **Role based access:** 6 access roles are provided in the Company system: test drive user, associate member, full member, researcher, Backoffice administratorand Site administrator.
3. **Account management policy:** Accounts use an email username and minimum 7 character length password with a minimum of 1 upper and 1 lower case letter.
4. **Remote access credentials management:** secure shell access is provided to server instances running in the Rackspace Cloud. Credentials are provided by the server system administrator.
5. **Separation of duties**: Programmers cannot access the production database. Only the DBA can access the production databases using the postgres user.
6. **Minimum privileges**: The application layer accesses production databases using a specific user (appuser) that has been granted minimum privileges to specific databases and IP address of the application server. This is implemented in the database schema and in the pg_hba.conf file that controls access at the PostgreSQL server level.

B) Automatic Session timeout (A) – Automated server session timeout after 30'
C) Encryption and Decryption (A) – ePHI is encrypted using PGP encryption inside the database engine in order to mitigate the risk of a data breach on the database server: idcode, name, initials, country, phone, skype, city, state_region

(2) Audit controls (R)

The Company maintains 4 levels of audit controls: application, table, server, O/S.

A) **Content of audit controls:** Application audit control is provided for user role, patient, test , subscription and online payment status change events. Table audit controls include create and modified timestamps on every row in every table after every transaction. Server audit controls are maintained by the PostgreSQL database and Apache2 servers.

Ubuntu 10.04 operating system audits are stored using standard syslog functions in /var/log.

B) **Audit reduction and report generation** – application level audit reports can be produced on demand by the application site admin. Server / OS level audit reports can be produced at any time from standard Ubuntu 10.04 /var/log files.

C) **Audit record retention**: Table audits: unlimited, server logs: 3 month retention, and application layer audit: unlimited.

D) **Unsuccessful logins**: marked in the operating system auth log

(3) Integrity

A) Mechanism to Authenticate Electronic Protected Health Information (A)

B) Person or Entity authenticate (R)

Accounts require an email username and minimum 7 character length password with a minimum of 1 upper and 1 lower case letter.

By default, database user passwords are stored as SHA-1 hashes, so the administrator cannot determine the actual password assigned to the user. Since SHA-1 encryption is used for database client authentication in the application server, the unencrypted password is never even temporarily present on the server because the client SHA-1 encrypts it before being sent across the network.

(4) Transmission security

A) Integrity Controls (A) – Particular attention is given to protection of data transmission between the client-side Flash test and the server. Data from the client is transmitted using AMF-encoded binary strings and data security is protected using one-time tokens. Every data transaction received by the application server from a Flash client tests the validity of the one-time token; if the token is invalid, the transaction is rejected by the server and a general warning notice provided. A crossdomain.xml policy file limits the client-side Flash test to exchange data only with the cpftest.com and moxo-adhdtest.com domains.

B) Encryption (A) – Browser-web server and web server-database server communications are encrypted with SSL. Administrative access is performed exclusively by SSH; no other services are provided on the servers.