Touchscreen Hearing Check

Data Security & Processes

Hearing Care Marketing

Background

Spinach Effect Solutions Pty Ltd, the inventor and licensor of the Touchscreen Hearing Check, has invested heavily in data handling and security processes to ensure that the solution is HIPAA compliant in the USA.

Protected Health Information (PHI)

The solution collects Protected Health Information (PHI) from Users, as defined by HIPAA Guidelines. Data collected includes, but is not limited to: first name; last name; email; phone; gender; age group; hearing check results, and User requests for further action.

Who owns Users' PHI?

Importantly, all PHI collected is 'owned' solely by the Client (Hearing Care Provider).

Spinach Effect Solutions Pty Ltd and our Distributors warrant to never resell or misuse any PHI.

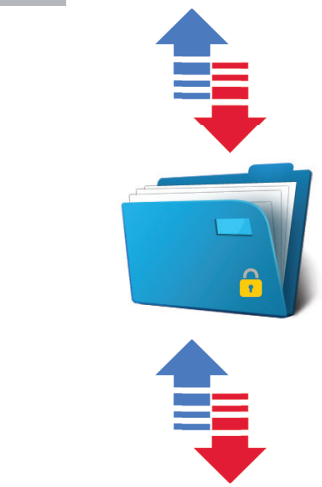
Data Encryption

Every Client utilizing the solution has a **unique public key,** which is automatically generated and is specific to their account.

The Client's unique Public Key is sent to the Hearing Touch Machine when it is registered to that Client's account.

This "key" is required to be able to read encrypted Protected Health Information (PHI) pertaining to Users of that Client's Touchscreen Hearing Check units. This includes:

- Data stored on the touchscreen tablet (i.e. iPad) when it is not connected to the Internet
- Data in transmission between iPads and the secure online Administration Portal
- Data stored within the Client's account on the secure Administration Portal



Touchscreen Hearing Check

All PHI stored on the Touchscreen Hearing Check during a 'live' hearing check is encrypted (256-bit) using the Client's own public key.

If the iPad is not connected to the Internet, PHI will be stored 'offline' until it is reconnected to the Internet and PHI can be securely transmitted to the Administration Portal.

Once PHI is transmitted successfully to the secure Administration Portal, it is deleted from the iPads.

No Protected Health Information can be extracted in a usable format from the Touchscreen Hearing Check.

Data transmissions

PHI is transmitted from iPads to the secure Administration Portal at the conclusion of the User's hearing check. Importantly, the system encrypts PHI during transmissions using 256-bit encryption and the Client's own public key.

Any PHI that is intercepted during data transmission to the Portal will be encrypted and unreadable.

Administration Portal

All PHI stored on our secure Administration Portal remains in encrypted with the Client's unique Public Key. Even if our servers were hacked, Users' ***Private Health Information*** would be unreadable. Furthermore:

1. Access to the Administration Portal is protected using client Usernames and Passwords, which limits access only to User data and Reports held under that client account.
2. The Administration Portal sends notifications of Users with hearing loss and their requests to your customer service email address
3. The Administration Portal also compiles and send Users their Free Hearing Reports

Spinach Effect Solutions Pty Ltd
p: +61 (0) 449 215 344 e: simon@hearingcaremarketing.com.au www.hearingcaremarketing.com.au