Face2Gene HIPAA Compliance Declaration

What is Face2Gene?
Face2Gene is a suite of phenotyping applications that facilitates comprehensive and precise genetic evaluations. FDNA uses facial analysis, deep learning and artificial intelligence to transform big data into actionable genomic insights to improve and accelerate diagnostics and therapeutics.

Background
With the rapid advance of healthcare technologies such as mobile medical apps and cloud computing and their increasing integration with social media such as Facebook – personal data protection has become of paramount importance.

The Centers for Medicare & Medicaid Services (CMS) provide guidance on Security Standards for the Protection of EPHI (Electronic Protected Health Information). This guidance is described in 45 CFR Parts 160 and 164 Subparts A and C and is commonly known as the Security Rule. The Security Rule implements provisions for data protection in HIPAA (Health Insurance Portability and Accountability Act).

Risk analysis
The first required safeguard in the Security Rule is a risk analysis – *"As part of the risk management process, the company performs an annual risk analysis for its products analyzing software and data security"*. The Security Rule details specific requirements for security safeguards. Items marked *(R)* are required and items marked *(A)* need to be addressed according to the results of the risk analysis.

To reduce risks to EPHI, covered entities and their business associates such as FDNA must implement the appropriate technical safeguards for their business situation – this is the raison d'être of risk analysis. The most effective safeguard is to store as little EPHI as possible. To this extent:

We collect the minimum necessary EPHI to ensure the proper use of Face2Gene. This EPHI may include: patient facial images or other uploaded patient files, case name, date of birth, date of visit, and case-related notes. These data types are stored in an encrypted file volume and are not accessible by other users of Face2Gene by default, unless explicitly and actively designated otherwise by the end-user. All digital communication links between users and the Face2Gene private cloud occurs over secure, encrypted communication protocols. An automatic learning algorithm is applied anonymously on EPHI stored in its FDNA's file volume in order to train and improve FDNA's Next-generation Phenotyping technologies. It is the users' responsibility to obtain appropriate consent from patients to upload EPHI into Face2Gene.

FDNA has performed a threat analysis of the Face2Gene mobile app and services. The threat analysis considered attack scenarios involving system availability, EPHI confidentiality, integrity and availability, as well as attacks on code and service configurations. The results of the threat analysis guide FDNA in their implementation of Security Rule safeguards.

Person or Entity authentication (R)
This safeguard requires a covered entity and its suppliers to *"Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed."* Authentication in FDNA ensures that a person is in fact who he or she claims to be before being allowed access certain features in Face2Gene. This is accomplished by providing satisfactory proof of identity, to attest that a new user is a healthcare professional. After completing the in-app registration, a new user is vetted by FDNA for use of the app. User authentication is based on an email username and strong passwords with a minimum of 7 characters, including at least 1 letter and 1 digit. New users claiming to be healthcare professionals that fail to pass FDNA's identity verification are assigned a limited Face2Gene account, wherein all information sharing features are disabled, until the unverified state is changed.

Access control
The Security Rule defines access as *"the ability or the means necessary to read, write, modify, or communicate data/information or otherwise use any system resource".*

FDNA has implemented access control in the Face2Gene system as follows:

1. Unique User Identification (R) – Unique user identification is provided for end users in the Face2Gene mobile app and for system administrators and software developers. Authentication and grant of access to Web services consumed by the handset app are performed using a token exchange protocol.
2. Emergency Access Procedure (R) – End users of the Face2Gene mobile app have an online password recovery procedure and can access their data via the mobile.
3. Automatic Logoff (A) – The mobile app automatically logs off after 48 hours of inactivity.
4. Encryption and Decryption (A) – EPHI (facial photographic images) is stored on encrypted server file volume.

Mobile device policy
In addition to Security Rule requirements for access control, FDNA realizes that innovative mobile apps such as Face2Gene are part of a diverse mobile IT environment that introduces new threats and requires appropriate security countermeasures. In the event a user has a lost or stolen mobile device, a user can de-authenticate the device remotely, through FDNA's support.

Users of Face2Gene are encouraged to use device-level security features such as requiring a password or PIN when the screen is turned on to provide an additional layer of protection.

In an enterprise network environment, FDNA enables IT departments of healthcare organization, such as hospitals to implement the following specific security countermeasures subject to their mobile device policy using MDM (mobile device management) software:

1. Controlled distribution and delivery of the Face2Gene app using a tool such as the Mobile Iron Enterprise App Storefront.
2. Remote Lock and Wipe that allows IT administrators to remotely remove sensitive data from the device.
3. Enable IT administrators to add/remove users and reset passwords.
4. Disable persistence of pictures on iOS local Storage (subject to mobile device security policy).

Such features require installing an enterprise version of Face2Gene under a separate license. To learn more about an enterprise license of Face2Gene, please contact support@fdna.com.

Audit controls

The Audit Controls safeguards require a covered entity to *"Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information."* FDNA maintains comprehensive audit logs on its cloud servers:

1. Content of audit controls: Access and all failed login attempts. System level messages such as scheduled job execution and mail server-related messages.
2. Audit reduction and report generation: Logs are retained and cycled through a 7 day retention cycle. Reports can be produced on demand.
3. Audit record retention: Logs cycle through a 7 day retention period.
4. Unsuccessful logins: Documented in auth.log.

Transmission security

Transmission security safeguards require a covered entity to: *"Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network."* These include:

1. Integrity Controls (A) -Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposal.
2. Encryption (A) – Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.

Face2Gene encrypts the connection between the mobile device and the cloud services using SSL (Secure sockets layer). The connection is encrypted using AES_256_CBC, with SHA1 for message authentication and DHE_RSA as the key exchange mechanism.

Summary

Face2Gene is a unique and innovative genetic search and reference mobile application, powered by the smart phenotyping technology. FDNA has implemented the appropriate Security Rule safeguards as part of a corporate commitment to protecting personal data through a strong security and compliance management program.

Updated August 20, 2018