Face2Gene EU Data Protection Compliance

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 EU Data Protection Directive and specifically, Article 29 Working Party (2007), Working Document on the processing of personal data relating to health in electronic health records (EHR), provide security standards for the protection of personal data and EHR. FDNA complies with EU law in addition to complying with US Security and Privacy standards described in 45 CFR Parts 160 and 164 Subparts A and C.

Adequate level of protection
The EU has recognized that the State of Israel provides an adequate level of protection for personal data as referred to in Directive 95/46/EC with regard to automated international transfers of personal data from the European Union to the State of Israel or, where those transfers are not automated, they are subject to further automated processing in the State of Israel. See http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32011D0061

Risk analysis
As a key part of the risk management process, the company performs an annual risk analysis for its products analyzing software and data security. The results of the risk analysis detail specific requirements for implementing appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, 150 Article 29 Working Party (2007), Working Document on the processing of personal data relating to health in electronic health records (EHR).

To reduce risks to EHR, FDNA implements 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 personal data as possible. To this extent:

Face2Gene does not store any type of EHR, such as name, address, dates and identifying numbers, other than facial photographic images, which may be uploaded if user has obtained an appropriate informed consent. Facial photographic images uploaded by users of Face2Gene are stored in an encrypted file volume on our servers in Ireland and are not accessible by other users of Face2Gene by default, unless explicitly and actively designated otherwise by the end-user. An automatic learning algorithm is applied anonymously on all facial photographic images stored in its Face2Gene file volume in order to train and improve the FDNA® Technology.

FDNA has performed a threat analysis of the Face2Gene application and services. The threat analysis considered attack scenarios involving system availability, personal data 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 data security and privacy safeguards.

Person or Entity authentication

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 Face2Gene ensures that a person is in fact who he or she claims to be before being allowed access to the application. This is accomplished by providing satisfactory proof of identity, to attest that a new user is a healthcare professional. After completing the registration, a new user is vetted by FDNA for use of the application. 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 new user's registration information is either authenticated or access is denied in its entirety and the new user's registration is cancelled.

Access control

Access control is "*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* - Unique user identification is provided for end users in Face2Gene 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* - End users of Face2Gene have an online password recovery procedure and can access their data via the web services or mobile app
3. *Automatic Logoff* – Face2Gene automatically logs off after 48 hours of inactivity.
4. *Encryption and Decryption* – personal data (facial photographic images) is stored on encrypted server file volume on our servers in Ireland.

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 a 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 specific security countermeasures subject to their mobile device policy using MDM (mobile device management) software

1. Controlled distribution and delivery of Face2Gene 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 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

FDNA Audit Controls safeguards 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 located in the Ireland:

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

FDNA Transmission security safeguards 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.

Transfer of data from the EU to the US

As necessary, FDNA uses "Standard Contract Clauses" (SCC), as determined by the EU data directives' model clauses, to enter into agreements in the EU (with sites and/or third party vendors) to ensure compliance with applicable EU data protection and privacy regulations for its EU users.

Breach notification

A new instrument for dealing with infringements of data security has been introduced in the data protection law of several European countries: the obligation of providers of electronic communications services to notify data breaches to the likely victims and to supervisory authorities. The purpose of data breach notifications to data subjects is to avoid damage: notification of data breaches and their possible consequences minimizes the risk of negative effects on the data subjects. FDNA has implemented appropriate internal procedures for breach notification; these are detailed in the company SOP (Standard operating procedure) for Incident Response.

Confidentiality
FDNA has implemented appropriate internal procedures to ensure that the secure processing of data is further safeguarded by the general duty on employees, to ensure that data remain confidential.

Data security officer
FDNA has appointed an internal data security officer as required by several European countries such as Germany.

Summary
Face2Gene is a unique and innovative genetic search and reference application, powered by smart phenotyping technology.

FDNA has implemented the appropriate safeguards to meet EU Data protection requirements as part of a corporate commitment to protecting personal data through a strong security and compliance management program.

If you have any questions or concerns, please send an email to support@fdna.com.

Updated 5 April, 2017