IAM eXchange
Annex A - Security commitment from the Trusted Platform

_____ (*)

Intents to offer Trusted Platform services as described in the service description. To offer this service with the right level of security,

_____ (*)

commits to respect following security rules:

(*): Company Name and CBE Nr

1.1 Business security

In case the development adds an additional use case based on an existing integration, the eHealth platform must be informed at least one month in advance with a detailed estimate of the expected load. This will ensure an effective capacity management.

In case of technical issues on the WS, the partner may obtain support from the contact center (see Chap 3)

In case the eHealth platform finds a bug or vulnerability in its software, we advise the partner to update his application with the newest version of the software within 10 business days.

In case the partner finds a bug or vulnerability in the software or web service delivered by the eHealth platform, he is obliged to contact and inform us immediately. He is not allowed to publish this bug or vulnerability in any case.

1.2 Level of Assurance

If the authentication method of at least one of the applications used by the Trusted Platform is higher than any other method, this higher method will be applied for accessing the Trusted Platform.

1.3 Communication

- All communications between the trusted platform and its views must be cryptographically protected (for example by using SSL). The protection must at least be on a transport level.
- Every communication with eHealth services must be compliant with the security policy of those services.
- The trusted platform must implement OpenId Connect protocol and obtain for each user an electronic assertion allowing to process data and call services in the same of that user for a limited time.
- Concerning the OpenId Connect protocol, the trusted platform is a confidential client. The TP will thus receive, protect, and use a cryptographic secret allowing it to authenticate itself to the OpenID Connect Provider whenever it requires a user token. The flow used is authorization code. The cryptographic secret a trusted platform receives is, along with the client ID, its key to the eHealth platform.

1.4 Delegation

- Assertions requested from the OpenId Connect provider are only issued if the end user is currently present, authenticated and expressed his consent on first use of the trusted platform during an interactive process. That consent process will take place within the OpenId Connect provider security context and inform the user of the trusted platform identity and what medical data the trusted platform will return and process. The user will be able to accept or refuse to consent.
- Subsequent requests will be honoured based on this explicit consent, as long as the consent itself is not revoked, and the user is still present and authenticated on the OpenId Connect provider.
- At any time and for any reason, a final user can list every trusted platform able to access his data, and revoke the previously granted consent for that platform.
- If a user does not use a trusted platform during a long period, the consent of that user and any assertion obtained from this consent can be revoked.
- A trusted platform must not (forbidden) ask the user for his eHealth platform credentials, key store or cryptographic keys. The only way allowed to perform operations in the name of a user is through the authorization code flow of the OpenId Connect provider (obtaining a signed token for that user).

1.5 Data

- The assertion allows the trusted platform to call eHealth services in the name of the final user. The trusted platform must then be able to secure access and storage of the assertion during their validity period.
- The trusted platform received a cryptographic secret during its enrolment process in order to authenticate any request to the OpenId Connect provider. That credential paired with their client ID is their digital key to the eHealth services. The trusted platform needs to secure storage and usage of those tokens. Authentication only happens through signed, short-validity tokens.
- The trusted platform must not (forbidden) store or cache any medical information longer than the time necessary for technical operations like interacting with the end-user or formatting the information. For example, the platform can have the information in session but never store it on a drive or database.
- Views must never (forbidden) persist any personal or medical data.
- Retention time of personal and medical data in memory must never exceed the validity period of the user's assertion that allowed retrieving those data.
- eHealth services requiring SAML Holder-of-Key (HOK) tokens do not understand the identity delegation semantics of the platform. If the trusted platform uses the Token Exchange Service in order to get such a legacy token from the OpenId provider token, then the trusted platform must take a privacy log containing the real identity of the caller every time the SAML HOK token is used.

1.6 Documentation

- Implementers of the trusted platform must provide a clear documentation of their infrastructure detailing the different views and technologies used, exchange protocols between their platform and their views, as well as governance and technical measures they implemented in order to protect the platform's cryptographic secret as well as the different end-users assertions during their validity period.

1.7 Incidents

- Any incident such as data leak, credential loss or compromise for platform or end-user must be immediately reported and disclosed to eHealth DPO (***dpo@ehealth.fgov.be***) so that counter-measures (such as revoking or rotating credentials) can be taken. Incident management will remain trusted platform's responsibility.

1.8   Security organisation

The partner supporting the trusted platform will take following organizational measures:

- Organization of information security : The organization will internally organize such that security is continuously measured and improved, information security incidents are detected, reported and remediated;
- Human resource security is organized;
- Access control (physical and logical) is implemented for every access to the resources of the trusted platform;
- Operation security is implemented (protection from malware, backup, logging, monitoring, …).

1.9   Revisions

The eHealth platform is constantly running risk assessments that can lead to changes, update, or new security requirements or controls. Trusted platform will receive information when such a change occurs.

The trusted platform commits to acts with due precautions and discernment to meet the aforementioned requirements in addition to the "minimal norms" as published on eHealth portal. Non-compliance can lead to the actual disconnection from eHealth services by suspension or revocation of its client ID.

Date of signature:	
Signature[1]**:**	
Name*:* *(The legal representative of the entity or the data security consultant)*	
First name	
Job title	

---

[1] *This document should be signed by a legal representative of the entity or by the information security consultant.*