HEALTH DATA HUB

PROCEDURE DE GESTION DES IDENTITES ET DES HABILITATIONS

Groupement d'Intérêt Public
« Plateforme des données de Santé »
9 rue Pitard, 75015 Paris
Tel : 01.45.18.43.90
Fax : 01.45.18.43.90

SOMMAIRE

1. Généralité

1.1. Objet du document

Le présent document précise les règles applicables pour assurer la sécurité des accès aux ressources dans le cadre des activités du Health Data Hub (HDH), ainsi que les principes de gouvernance associés.

1.2. Responsabilité et processus de validation de la procédure

1.2.1. Rédaction de la procédure

La procédure de gestion des identités et des habilitations est rédigée par le RSSI.

1.2.2. Validation de la procédure

La procédure de gestion des identités et des habilitations est validée par le RSSI, le Directeur Technique et le DPD.

1.3. Périmètre

1.3.1. Périmètre d'application

La procédure de gestion des identités et des habilitations doit être mise en œuvre sur l'ensemble des systèmes d'information du HDH, à savoir :

- Le matériel informatique et les applications mis à disposition des Agents et Externes sous contrat dans le cadre de la réalisation de leurs missions au sein du HDH, appelé « **Équipement et applications informatiques** », d'une part ;
- La plateforme technologique du HDH, appelée « **Plateforme** », d'autre part.

Les principes généraux s'appliquant aux deux SI sont indiqués en début de chaque partie. Ceux spécifiquement liés à l'un des deux SI sont différenciés par le code couleur dédié à son SI, comme expliqué ci-dessous :

- Principe général -

Équipement et applications informatiques	*- Principe spécifique à l'Équipement et applications informatiques e -*
Plateforme	*- Principe spécifique à la Plateforme -*

1.3.2. Population concernée

La population concernée par l'application de cette procédure est l'ensemble des Agents et Externes sous contrat du HDH, les utilisateurs de la **Plateforme**, l'ensemble des utilisateurs des SI du HDH, ainsi que toute personne physique ou morale tierce intervenant sur les SI du HDH (fournisseurs, prestataires de services, sous-traitants, etc.).

2. Gestion des identités

La gestion des identités désigne toutes les activités ayant pour but d'établir l'identité des utilisateurs qui accèdent aux ressources du HDH. Cela comprend le contrôle de la validité des informations et la gestion du cycle de vie des identités : arrivée, départ et mouvement.

Le processus de gestion des identités du SI du HDH est basé sur le cycle de vie des identités, prenant en compte les arrivées et départs des utilisateurs des SI.

2.1. Règles générales de gestion des identités

Plusieurs règles sont à appliquer dans la gestion des identités sur le SI du HDH:

- Toute demande de création d'identité doit être réalisée par un référent habilité (RH, supérieur hiérarchique, responsable de contrat pour les prestataires et Autorité d'Enregistrement pour les utilisateurs externes de la **Plateforme**) par mail à l'opérateur concerné.
- L'opérateur concerné est en charge de vérifier la légitimité de la demande auprès des acteurs adéquats (ils sont définis dans les procédures opérationnelles de gestion des arrivées pour chaque population) avant de créer l'identité.
- La traçabilité de la demande doit être garantie (conservation des mails de demande et de validation si existants).
- Un registre des identités créées doit être mis en place et tenu à jour. Il peut être mis en place par type de SI si nécessaire. Ce registre doit contenir a minima la date de création du compte, le SI concerné, le nom du référent et les informations de l'utilisateur.
- Les identités des Externes sous contrat doivent indiquer une date d'expiration. Si la durée n'est pas précisée par le demandeur, elle doit être de 6 mois. Cette date d'expiration est à indiquer dans le registre et à paramétrer dans le SI concerné lorsque cela est techniquement possible.
- Le référent doit signaler tout départ au plus tôt à l'opérateur concerné.
- Chaque action (enregistrement, modification, suppression, désactivation, etc.) réalisée sur une identité doit être journalisée (identité modifiée, identité de la personne réalisant l'action, type d'action, date et heure de l'action) et ce pour des raisons de traçabilité.

2.2. Rôles et responsabilités dans le cadre du processus d'arrivée

Les processus d'arrivée des utilisateurs sont décrits dans les procédures dédiées pour chaque type de population.

Les responsabilités autour de la gestion des identités dans le cadre de l'arrivée d'un utilisateur sont indiquées ci-dessous.

2.2.1. Agents et externes sous contrat

Action	Responsable	
	Équipement et applications informatiques	**Plateforme**

Demande de création d'un nouvel utilisateur	Responsable hiérarchique ou responsable de contrat	Responsable des opérations
Création de l'identité dans le référentiel d'identité	Opérateur équipement informatique	Opérateur plateforme

2.2.2. Utilisateurs projets externes

Action	Responsable	
	Équipement et applications informatiques	**Plateforme**
Demande de création d'un nouvel utilisateur	Responsable des opérations	Autorité d'enregistrement du responsable de traitement
Création de l'identité dans le référentiel d'identité	Opérateur équipement informatique	Opérateur plateforme

2.3. Rôles et responsabilités dans le cadre du processus de départ

Les processus de départ des utilisateurs sont décrits dans les procédures dédiées pour chaque type de population.

Les responsabilités autour de la gestion des identités dans le cadre du départ d'un utilisateur sont indiquées ci-dessous.

2.3.1. Agents et externes sous contrat

Action	Responsable	
	Équipement et applications informatiques	**Plateforme**
Demande de désactivation de compte suite au départ d'un utilisateur	Responsable hiérarchique ou responsable de contrat	Responsable des opérations
Désactivation de l'identité dans le référentiel d'identité	Opérateur Équipement informatique	Superopérateur
Suppression des droits	Opérateur Équipement informatique	Superopérateur

Mise en quarantaine dans une unité d'organisation spécifique	Opérateur Équipement informatique	Superopérateur
Suppression de l'identité dans le référentiel d'identité après un an	Opérateur Équipement informatique	Superopérateur

2.3.2. Utilisateurs projets externes

Action	Responsable	
	Équipement et applications informatiques (compte Slack)	Plateforme
Demande de désactivation de compte suite au départ d'un utilisateur	Responsable des opérations	Autorité d'enregistrement du responsable de traitement
Désactivation de l'identité dans le référentiel d'identité	Opérateur équipement informatique	Opérateur projet
Suppression des droits	Opérateur équipement informatique	Opérateur projet
Mise en quarantaine dans une unité d'organisation spécifique	Opérateur équipement informatique	Opérateur plateforme
Suppression de l'identité dans le référentiel d'identité après un an	Opérateur équipement informatique	Opérateur plateforme

3. Gestion des habilitations

La gestion des habilitations désigne toutes les activités ayant pour but d'assurer que tous les utilisateurs accèdent aux SI du HDH en cohérence avec leur fonction.

Ceci comprend :

- La définition du modèle d'habilitation ;
- L'attribution des profils aux utilisateurs ;
- Le provisionnement des droits associés aux profils dans les cibles techniques.

3.1. Règles générales de gestion des habilitations

Plusieurs règles sont à appliquer dans la gestion des habilitations sur le SI du HDH :

- Les principes du moindre privilège et de la limitation des privilèges doivent être observés pour toute habilitation donnée. Une habilitation ne doit être donnée que si elle est requise et adaptée au poste de l'utilisateur.
- Chaque actif du SI du HDH est sous la responsabilité d'un "Responsable de Ressource" qui est responsable des habilitations attribuées sur cet actif.

Plateforme	Le Responsable de Ressource de la plateforme technologique est le Directeur Technique.

- Toute demande d'habilitation pour un utilisateur doit être validée a minima par son référent (responsable hiérarchique, responsable de contrat ou autorité d'enregistrement) ainsi que le Responsable de Ressource sur lequel l'habilitation est attribuée.
- Les demandes d'habilitations ainsi que les validations doivent êtres conservées pour des besoins de traçabilité.
- Les Responsables de Ressource identifiés pour chaque SI ou répertoire du HDH sont en charge de maintenir à jour une liste des habilitations attribuées sur leur périmètre.
- La liste des Responsables de Ressource est tenue à jour par la Direction Technique.
- Lorsque le SI concerné le permet, les habilitations sont attribuées au travers de groupes d'accès et non de manière unitaire à chaque utilisateur afin de faciliter les actions de maintien à jour des habilitations.
- Lorsque le SI concerné le permet, les habilitations sont attribuées aux utilisateurs au travers de profils (exemple: profil utilisateur projet X, profil utilisateur équipe Fabrique, etc.) et non au travers de droits unitaires afin de faciliter les modifications d'habilitation et les actions de contrôle.
- La traçabilité des actions de modification des habilitations doit être garantie.

3.2. Gestion du modèle d'habilitation

Un modèle d'habilitation est défini et tenu à jour pour chaque SI du HDH. Chaque Responsable de Ressource a la responsabilité du maintien à jour de ce modèle pour sa ressource.

Le tableau ci-dessous présente les responsables en charge de la gestion du modèle d'habilitation.

Action	Responsable	
	Équipement et applications informatiques	**Plateforme**
Identification du besoin de création/suppression d'un profil, et identification des droits qui lui sont attribués	Responsable de Ressource concernée	Directeur technique
Validation de la création / suppression du rôle	Responsable de Ressource concernée	RSSI
Implémentation / Suppression du rôle	Responsable de Ressource concernée ou Opérateur équipement informatique	Opérateur plateforme

Plateforme	Le détail des habilitations de chaque profil d'opération de la plateforme est présent dans le dossier d'architecture technique générale.

3.3. Attribution des habilitations

Une fois l'identité créée, un ou plusieurs profils lui sont attribués. Les responsabilités sont listées ci-dessous.

3.3.1. Agents et externes sous contrat

Action	Responsable	
	Équipement et applications informatiques	**Plateforme**
Validation de l'attribution d'un profil	Responsable hiérarchique ou responsable de contrat et Responsable de Ressource concernée	Responsable des opérations

Attribution d'un profil	Responsable de Ressource concernée ou Opérateur équipement informatique	Superopérateur

Plateforme	Une personne ne peut disposer de plus d'un rôle d'opération de la Plateforme.

3.3.2. Utilisateurs projets externes

Action	Responsable	
	Équipement et applications informatiques	**Plateforme**
Validation de l'attribution d'un profil à un utilisateur	Responsable des opérations et Responsable de Ressource concernée	Autorité d'enregistrement de l'organisme porteur du projet
Attribution d'un profil à l'utilisateur	Responsable de Ressource concernée ou Opérateur équipement informatique	Opérateur projet

Le provisionnement désigne le fait de transmettre les habilitations attribuées dans le référentiel d'identité aux ressources cibles. Ainsi, les utilisateurs demandent et se voient attribuer des habilitations dans le référentiel d'identité, qui se charge ensuite de les transmettre aux différentes ressources.

4. Gestion du contrôle d'accès

4.1. Règles générales sur le contrôle d'accès

[redacted]

4.1.1. Règles spécifiques liées aux mots de passe

[redacted]

[redacted]

4.2. Attribution des secrets d'authentification

[redacted]

4.3. Renouvellement des secrets d'authentification

[redacted]

[redacted]	[redacted]

5. Règles pour la gestion des comptes à privilèges

[redacted]

[redacted]

6. Contrôles

6.1. Recertification des accès au SI du HDH

[redacted]

[redacted]

[redacted]	[redacted]
[redacted]	[redacted]