RÈGLES D'ACCÈS À L'ENTREPÔT DE DONNÉES DE SANTÉ (EDS)DE L'AP-HP À DES FINS DE RECHERCHE

Validées par le Comité de Pilotage Stratégique de l'EDS le 01/07/2020 et la Commission Médicale d'Établissement de l'AP-HP le

Contenu

Article 1 - Liste des abréviations

CSE	Comité Scientifique et Éthique de l'Entrepôt de Données de Santé de l'AP-HP
CME	Commission Médicale d'Établissement de l'AP-HP
CMEL	Commission Médicale d'Établissement Locale du GHU AP-HP
DIM	Département d'Information Médicale AP-HP
DRCI	Direction de la Recherche Clinique et de l'Innovation de l'AP-HP
DSI	Direction des Systèmes d'Information de l'AP-HP
EDS AP-HP	Entrepôt de Données de Santé de l'AP-HP
URC	Unité de Recherche Clinique de la DRCI de l'AP-HP

Article 2 - Glossaire

Recherche interne dite « équipe de soins »	Recherche réalisée à partir des seules données ou échantillons recueillis dans le cadre des soins, par les professionnels de santé ayant participé à la prise en charge du patient.
Recherche multicentrique dite « hors équipe de soins »	Recherche répondant à au moins l'une des conditions suivantes : - Le responsable et toutes les personnes associées à la recherche (sauf personnels AP-HP des URC / Santé Publique / DIM / DSI intervenant en soutien à la recherche) n'ont pas participé à la prise en charge de la totalité de patients inclus - La recherche est réalisée à partir des données recueillies lors d'une précédente recherche - La recherche implique un partenaire externe à l'AP-HP
Pseudonymisation	Technique qui consiste à remplacer un identifiant (ou plus généralement des données à caractère personnel) par un pseudonyme. La pseudonymisation permet ainsi de traiter les données d'individus sans pouvoir identifier ceux-ci de façon directe.
Entrepôt de Données de Santé (EDS)	Base de données constituée à partir des données relatives aux patients pris en charge à l'AP-HP et dont l'exploitation s'appuie techniquement sur la Plateforme Données Massives AP-HP (ressources de calculs distribués, outils d'analyse, etc.).

Article 3 - Conditions d'accès à l'EDS à des fins de recherche

a) Règles générales

- L'EDS est accessible à tous les personnels de l'AP-HP souhaitant mettre en œuvre des projets de recherche en santé.
- Pour être habilités à accéder aux données de l'EDS, les personnels de l'AP-HP doivent préalablement :

  - Suivre une formation aux outils permettant l'exploitation des données de l'EDS (inscription auprès des coordinateurs EDS dont les coordonnées figurent en Annexe 3)
  - S'engager par écrit, à l'issue de la formation, à respecter les présentes règles et la charte de bon usage du système d'information de l'AP-HP (annexe 16 du règlement intérieur de l'AP-HP)
- Le responsable de la recherche doit informer les professionnels de santé impliqués dans la prise en charge des patients concernés par la recherche ou ayant contribué à la production des données qui seront utilisées (recherche interne ou multicentrique), en fonction de la thématique et du périmètre de la recherche : les collégiales de l'AP-HP, les responsables recherche des DMU, les chefs de service, les équipes médicales, les coordinateurs des filières de santé maladies rares ou des centres de référence, etc.
- Dans le cadre d'une recherche multicentrique, cette information doit être réalisée par le responsable de la recherche en amont du dépôt du projet de recherche au Comité Scientifique et Ethique (CSE) de l'EDS
- En complément, pour les recherches multicentriques ayant reçu un avis favorable du CSE, celui-ci informe les représentants des professionnels de santé impliqués dans la prise en charge des patients concernés par la recherche ou ayant contribué à la production des données utilisées en les renvoyant vers le site internet de l'EDS (https://eds.aphp.fr/) : les collégiales de l'AP-HP, les responsables recherche des DMU, les représentants hospitalo-universitaires des CMEL
- Les professionnels de l'AP-HP s'engagent à :
  - Utiliser les données strictement nécessaires aux recherches
  - Réaliser les traitements de données sur les serveurs de l'AP-HP (postes de travail AP-HP ou procédures d'accès à distance sécurisées de VPN mises en œuvre par l'AP-HP)
  - Ne pas transférer ces données sur des supports mobiles (clefs USB, disques durs, etc.). Si les données doivent temporairement être stockées sur des supports mobiles, ceux-ci doivent présenter des garanties de sécurité suffisantes (mot de passe, chiffrement, etc.) et un argumentaire justifiant la nécessité de ce stockage temporaire doit être soumis à l'avis du CSE
  - Ne pas croiser ces données avec des données d'autres sources (fichiers, bases de données) en dehors des besoins d'une recherche ayant obtenu un avis favorable du CSE et de la CNIL
  - Avertir le délégué à la protection des données (DPO) à l'adresse protection.donnees.dsi@aphp.fr en cas d'incident relatif à la confidentialité et la sécurité des données
  - Ne pas tenter de ré-identifier les patients dont les données de santé sont accessibles au sein de l'échantillon mis à disposition

b) Règles spécifiques aux recherches internes dites « équipe de soins »

- Les professionnels de santé peuvent mettre en œuvre des recherches internes dites « équipe de soin » dans les conditions suivantes :
  - Informer le responsable de l'équipe de soins
  - Contacter le référent protection des données pour établir la conformité du traitement, et le faire inscrire au registre général des traitements de l'AP-HP
  - Réaliser les traitements de données sur la Plateforme Données Massives de l'AP-HP ou sur un équipement inventorié par l'AP-HP
  - Partager les données individuelles de santé avec les seules personnes ayant participé à la prise en charge des patients concernés par la recherche
  - Ne pas croiser ces données avec d'autres bases de données
  - Si les données doivent temporairement être stockées sur des supports mobiles (clefs USB, disques durs, etc.), ceux-ci doivent présenter des garanties de sécurité suffisantes (mot de passe, chiffrement, etc.) validées par le DPO
  - Procéder à la destruction de toutes données sur les équipements et supports mobiles dès lors qu'il n'y a plus nécessité d'en disposer dans le cadre de la recherche
  - Avertir le délégué à la protection des données à l'adresse protection.donnees.dsi@aphp.fr en cas d'incident relatif à la confidentialité et la sécurité des données ;

  - Mentionner dans toute publication issue de ces travaux : « Cette recherche a bénéficié du soutien des équipes en charge de l'Entrepôt de Données de Santé de l'Assistance Publique – Hôpitaux de Paris (AP-HP) » « This research was supported by the teams in charge of the Clinical Data Warehouse of Greater Paris University Hospitals (AP-HP) »
  - Respecter, dans toute publication issue de ces travaux, les règles d'affiliation aux structures hospitalières de la charte de signature de l'AP-HP (Annexe 1)
- Si des manquements à ces engagements venaient à être constatés :
  - Le délégué à la protection des données de l'AP-HP pourra être saisi
  - En cas de manquement grave, susceptible de porter préjudice aux personnes concernées par le traitement et/ou à l'institution, les auteurs s'exposent à des sanctions disciplinaires et des poursuites pénales.

c) Règles spécifiques aux recherches multicentriques dites « hors équipe de soin »

- Les professionnels de santé peuvent mettre en œuvre des recherches multicentriques dans les conditions suivantes :
  - Réaliser le traitement, par défaut, sur des données pseudonymisées et au sein de la Plateforme Données Massives hébergée à l'AP-HP
  - S'assurer de la conformité réglementaire de la recherche avec une URC de la DRCI
  - Si la recherche n'entre pas dans le cadre d'une des méthodologies de référence de la CNIL, mettre à disposition du CSE les documents d'autorisation de la CNIL une fois celle-ci obtenue
  - Avoir reçu l'avis favorable du CSE
  - Contacter la DRCI (URC) pour procéder à l'inscription de la recherche au registre général des traitements de l'AP-HP
  - Ne pas tenter de ré-identifier les patients dont les données individuelles de santé sont comprises dans l'échantillon mis à disposition
  - Avertir le délégué à la protection des données à l'adresse protection.donnees.dsi@aphp.fr en cas d'incident relatif à la confidentialité et la sécurité des données.
  - Mentionner dans toute publication issue de ces travaux : « Cette recherche a bénéficié du soutien des équipes en charge de l'Entrepôt de Données de Santé de l'Assistance Publique – Hôpitaux de Paris (AP-HP) » « This research was supported by the teams in charge of the Clinical Data Warehouse of Greater Paris University Hospitals (AP-HP) »
  - Respecter, dans toute publication issue de ces travaux, les règles d'affiliation aux structures hospitalières de la charte de signature de l'AP-HP (Annexe 1)

- Si des manquements à ces engagements venaient à être constatés :
  - Le délégué à la protection des données pourra être saisi
  - L'accès à l'EDS pourrait être interdit pendant une durée proportionnelle à la gravité du manquement
  - Les directeurs de publication des revues médicales ayant publié les travaux pourraient être saisis
  - En cas de manquement grave, susceptible de porter préjudice aux personnes concernées par le traitement et/ou à l'institution, les auteurs s'exposent à des sanctions disciplinaires et des poursuites pénales

d) Accompagnement méthodologique et technique

Les professionnels des URC de la DRCI, de la DRCI centrale, des Départements de Santé Publique, des DIM, et de la DSI centrale ont accès aux données pseudonymisées afin d'assurer un support méthodologique et/ou technique à la recherche. Ils s'engagent à :

- Utiliser les données strictement nécessaires aux recherches
- Réaliser les traitements de données sur les serveurs de l'AP-HP : postes de travail AP-HP ou procédures d'accès à distance sécurisées de VPN mis en œuvre par l'AP-HP

- Ne pas transférer ces données sur des supports mobiles (clefs USB, disques durs, etc.). Si les données doivent temporairement être stockées sur des supports mobiles, ceux-ci doivent présenter des garanties de sécurité suffisantes (mot de passe, chiffrement, etc.)
- Ne pas croiser ces données avec des données d'autres sources (fichiers, bases de données) en dehors des besoins d'une recherche ayant obtenu un avis favorable du CSE et de la CNIL
- Permettre l'accès aux données aux seules personnes habilitées dans le cadre des projets de recherche en appui desquels ils interviennent
- Avertir le délégué à la protection des données à l'adresse protection.donnees.dsi@aphp.fr en cas d'incident relatif à la confidentialité et la sécurité des données.
- Ne pas tenter de ré-identifier les patients dont les données de santé sont comprises dans l'échantillon mis à disposition

Les professionnels des URC accèdent aux données pseudonymisées de l'EDS pour :

- Évaluer la faisabilité des projets de recherche avant leur soumission à l'avis du CSE
- Préparer des réponses aux appels à projets
- Exécuter les requêtes de création des vues multicentriques permettant la mise à disposition de l'échantillon de données nécessaire à la recherche
- Participer aux traitements des données
- Participer à la rédaction des rapports d'analyse

Dans le cadre de leurs missions respectives, les personnels de la DSI centrale sont susceptibles d'accéder aux données directement identifiantes de l'EDS, dans le respect du secret professionnel, pour les seules fins suivantes :

- Intégrer les données dans l'EDS
- Préparer les données nécessaires à la mise en œuvre d'une recherche en santé
- Développer et qualifier les composants techniques et les solutions applicatives de la Plateforme Données Massives AP-HP
- Constituer et mettre à disposition les échantillons de données nécessaires aux recherches ayant obtenu un avis favorable du CSE

- Contribuer au contrôle de la qualité de ces échantillons de données et à leur enrichissement le cas échéant
- Archiver ou supprimer les données dont les délais de conservation ont expiré
- Exclure les données personnelles des patients qui se sont opposés à leur réutilisation à des fins de recherche

e) Partenaires extérieurs à l'AP-HP

- Les projets de recherche en santé de la Plateforme Données Massives AP-HP peuvent impliquer un partenaire extérieur, à l'exclusion des sociétés d'assurances et organismes financiers
- Lorsqu'une recherche implique un partenaire extérieur, un professionnel de santé de l'AP-HP doit nécessairement y être associé et, sauf exception, être le responsable de la recherche (investigateur coordinateur)
- Toute recherche associant un partenaire extérieur fait l'objet d'un contrat préparé par la DRCI et signé par les parties prenantes, incluant une clause relative à la protection des données
- Les partenaires extérieurs s'engagent à respecter les présentes règles.

f) Conditions particulières en cas de transfert de données de l'EDS vers des systèmes tiers

Les traitements sont réalisés par défaut sur des données pseudonymisées et au sein de la Plateforme Données Massives hébergée à l'AP-HP.

Toutefois, un transfert de données aux partenaires extérieurs de l'AP-HP peut être envisagé sous réserve du respect de l'ensemble des conditions suivantes :

- Présenter un argumentaire justifiant la nécessité de ce transfert au CSE
- Obtenir un avis favorable du CSE
- Faire valider la demande d'export auprès du Comité de Pilotage Stratégique de l'EDS
- Faire valider les modalités de mise en œuvre du traitement de données à caractère personnel par le Délégué à la Protection des Données de l'AP-HP
- Établir un contrat entre l'AP-HP et le(s) partenaire(s), incluant une clause relative à la protection des données

Article 4 - Habilitation des utilisateurs

Le processus de gestion des habilitations des personnes, pour l'accès aux données et aux applications de l'EDSR, se trouve en Annexe 2 « Procédure de gestion des comptes de l'EDS Recherche ». La version en vigueur a été communiquée à la CNIL le 28 avril 2020.

Pour chaque projet de recherche adressant les données de l'EDS qui lui est soumis, le Comité scientifique et éthique (CSE) est également destinataire de la liste nominative des personnes habilitées à accéder à une partie des données de l'EDS à cette fin.

Article 5 - Information des patients

Des affiches d'information sont apposées dans les lieux d'accueil du public des différents établissements de l'AP-HP. Une version en français et une version en anglais sont disponibles.

Un site Internet de transparence https://eds.aphp.fr/ est maintenu à jour et recense l'ensemble des recherches multicentriques hors « équipes de soin » ayant reçu avis favorable du CSE, conformément aux articles 13 et 14 du Règlement Général sur la Protection des Données (RGPD). Le site informe les patients de l'utilisation de leurs données de santé à des fins de recherche et de la possibilité de s'opposer à cet usage, à tout moment et sans se justifier, en s'adressant au directeur de l'hôpital où ils ont été pris en charge ou en remplissant le formulaire d'opposition électronique disponible sur le site internet de l'EDS.

Cette information figure également dans les livrets d'accueil du patient hospitalisé, en bas des comptes rendus de consultation et d'hospitalisation, et dans la charte de la personne hospitalisée.

En vue de la publication sur le site internet de l'EDS par le secrétariat du CSE, le responsable de la recherche communique :

- Le titre de la recherche
- Le résumé en français en langage clair et compréhensible
- Le cas échéant, les résultats de leurs recherches
- Le responsable de traitement des données
- L'acteur opérationnel
- Le sous-traitant
- Les finalités
- Les catégories de données traitées
- Le chaînage des données avec le SNDS
- Les destinataires des données
- Le transfert de données hors UE
- La date de mise en œuvre du traitement
- La durée de conservation
- Les modalités d'exercice des droits

Le site aphp.fr propose également une information relative à la protection des données à caractère personnel : https://www.aphp.fr/protection-des-donnees-personnelles

Annexe 1 : Charte de signature de l'AP-HP

Afin de pouvoir recenser l'ensemble des publications des auteurs de l'AP-HP dans les analyses bibliométriques internationales et de valoriser la forte contribution du CHU francilien aux activités de recherche biologiques, pré cliniques et cliniques, l'affichage et la visibilité des institutions auxquelles sont affiliés les auteurs sont fondamentaux.

La signature des publications scientifiques dans les revues internationales à comité de lecture doit être homogénéisée et permettre à coup sûr d'identifier les institutions d'origines des signataires.

COMMENT SIGNER SA PUBLICATION

Dans le domaine de la signature des publications scientifiques, tous les partenaires de la recherche s'accordent pour que les mêmes règles s'appliquent à l'ensemble des auteurs.

Que la publication soit liée directement ou indirectement à une activité de recherche financée, organisée et promue par l'Assistance Publique-Hôpitaux de Paris ou réalisée dans le cadre d'études organisées et financées partiellement ou totalement par d'autres hôpitaux ou organismes (Universités, Inserm, CNRS, etc.), chacune de ces institutions doit être identifiée sur une même ligne (modèle mono ligne de la charte AVIESAN 2016).

Une ligne d'adresse comporte les éléments suivants et dans l'ordre indiqué :

1 - Nom de l'Université d'appartenance, le cas échéant

2 – AP-HP

3 - Nom de l'hôpital ou de l'unité de recherche

4 – DMU (facultatif)

5 – Autre organisme ou institution d'affiliation

6 – Ville

7 - Code postal

8 – Pays

EXEMPLES DE SIGNATURES POUR L'AP-HP (MONO ET MULTI-TUTELLES)

• A Dupond

AP-HP, Hôpital Ambroise Paré, IMAGERIE MED NUCL, Boulogne, France

• L. Dupont

Université de Paris, AP-HP, Hôpital Lariboisière, DMU INVICTUS, BIOSCAR UMRS 1132, INSERM, Paris, France

• J-L. Durand

Sorbonne Université, UPRES EA 2397, AP-HP, Hôpital Pitié-Salpêtrière, Service de Pneumologie, Paris, France

Annexe 2 : Procédure de gestion des comptes de l'EDS Recherche de l'AP-HP

Version en vigueur communiquée à la CNIL le 28 avril 2020

Objet

Formaliser et sécuriser le processus de gestion des accès aux 3 applications de l'EDS RECHERCHE :

- **I2b2**, solution open source permettant de constituer des cohortes de patients et de construire des environnements de travail sécurisés avec les données nécessaires, mises à disposition pour chaque projet de recherche
- **Jupyter**, application web dédiée à l'analyse de données massives permettant de programmer dans plusieurs langages (Python, R, Scala, etc.)
- **Cohort360**, outil de visualisation et de constitution de cohortes de patients

Domaine d'application

Entrepôt de données de santé de l'AP-HP.

Glossaire

EDS = Entrepôt des Données de Santé de l'AP-HP

EDSR = Entrepôt des Données de Santé de l'AP-HP pour la finalité recherche

GHU = Groupe Hospitalo-Universitaire

DMU = Département Médico-Universitaire (ancien pôle)

DSI = Direction des systèmes d'information

PGSSI = Politique générale de sécurité des systèmes d'information

DIM = Département d'information médicale

URC = Unité de Recherche Clinique

DRCI = Délégation de la Recherche Clinique et de l'Innovation

OMOP = Observational Medical Outcomes Partnership, modèle relationnel de bases de données de santé, qui a pour objectif l'interopérabilité entre les différentes bases d'analyse en santé, qu'elles soient cliniques ou médico-administratives (https://www.ohdsi.org/data-standardization/the-common-data-model/)

Textes de référence

- Règlement général sur la protection des données, avril 2016, Loi Informatique et Libertés, Code de la santé publique
- Charte de bon usage du système d'information de l'AP-HP, Version 2.0, janvier 2016
- Guide méthodologique pour l'auditabilité des SI : Fiabilisation et certification des comptes des établissements publics de santé - Direction générale de l'offre de soins, janvier 2013

Description

I. Désignation des référents EDS

La gestion des accès à l'EDS est réalisée différemment pour chacune des trois applications Jupyter, i2b2 et Cohort360. Des référents EDS sont missionnés dans chaque GHU pour gérer les accès des utilisateurs (création / modification / désactivation) conformément aux stricts besoins métiers de l'utilisateur et aux règles d'attribution des droits. Les référents EDS sont issus des personnels des DIM, URC, Santé Publique et DSI locale. S'agissant de Cohort360, ces référents EDS peuvent gérer localement les comptes utilisateurs. Pour i2b2 et Jupyter, la gestion des comptes est centralisée à la DSI centrale, et les référents transmettent aux administrateurs les fichiers de paramétrage (cf. annexe « 006.3 EDSR - Modele_recueil_utilisateurs »). Une fiche de mission est transmise au coordinateur de chaque GHU (cf. annexe « 006.4 EDSR - Fiche mission coordinateur »).

II. Gestion des droits d'accès

Le référent EDS dispose d'un référentiel et/ou d'une matrice des droits sur lesquels il s'appuie pour assurer la gestion des accès dont il a la responsabilité (cf. annexe « 006.2 EDSR - Matrice des habilitations »). Les utilisateurs sont classés en neuf grandes catégories auxquelles sont associés un ou plusieurs métiers :

- **Catégorie1 : Personnel de santé d'une équipe de soin et assimilés**
  - Métier1 : Personnel médical
  - Métier2 : Personnel paramédical
  - Métier3 : IRC Ingénieur de recherche clinique (chef de projet)
- **Catégorie2 : Personnel d'un Département d'Information Médicale (DIM) local**
  - Métier1 : Personnel médical
  - Métier2 : Référent EDS
  - Métier3 : Ingénieur informatique DIM
- **Catégorie3 : Personnel du Département d'Information Médicale (DIM) central**
  - Métier1 : Personnel médical
  - Métier2 : Référent EDS
- **Catégorie4 : Personnel autorisé par un protocole d'étude (utilisateur final) = équipe de recherche (ex. recherche multicentrique validée par le comité Scientifique et Ethique (CSE))**
  - Métier1 : Personnel médical
  - Métier2 : Personnel paramédical
  - Métier3 : Equipe de recherche
  - Métier4 : Datascientist
  - Métier5 : Biostatisticien
- **Catégorie5 : Personnel de la Délégation de la Recherche Clinique et de l'Innovation (DRCI)**
  - Métier1 : Référent EDS
- **Catégorie6 : Personnel d'une Unité de Recherche Clinique (URC)**
  - Métier1 : Personnel médical
  - Métier2 : Référent EDS
  - Métier3 : Datascientist
  - Métier4 : IRC Ingénieur de Recherche Clinique (chef de projet)
  - Métier5 : Assistant de Recherche Clinique (ARC)
  - Métier6 : Technicien de d'Etude Clinique (TEC)
- **Catégorie7 : Personnel d'un service de Santé Publique**
  - Métier1 : Personnel médical
  - Métier2 : Référent EDS
  - Métier3 : Biostatisticien
- **Catégorie8 : Personnel de la Direction des Système d'Information (DSI)**
  - Métier1 : Ingénieur informaticien
- **Catégorie9 : Personnel de la Direction des Système d'Information Locale (DSIL)**
  - Métier1 : Ingénieur informaticien

Les catégories d'utilisateurs et les métiers présentés ci-dessus seront amenés à évoluer au cours du déploiement des applications de l'EDS et de l'utilisation de la plateforme par de nouveaux personnels.

Des **profils d'accès**, détaillés dans la suite du document, sont définis pour chaque application. Ils précisent les droits qui peuvent être alloués à un utilisateur. Un profil d'accès est attribué par défaut à chacun des métiers décrits ci-dessus (cf. annexe « 006.2 EDSR - Matrice des habilitations »). Dans certains cas, le profil d'accès d'un utilisateur peut être adapté par rapport au profil par défaut de son métier. Les comptes administrateurs sont limités à un nombre restreint d'agents et une revue régulière de l'activité de ces comptes est effectuée.

a. Création

Une création de compte est réalisée lorsqu'une personne habilitée demande à avoir accès à l'un des logiciels de l'EDS. Chaque demande de création d'un accès est formalisée et validée (cf. annexe «006.3 EDSR - Modele_recueil_utilisateurs »). La création des accès est tracée à l'aide d'un système de journalisation.

b. Modification

Une modification d'un compte a lieu lors d'un changement d'affectation ou d'un changement de niveau de droit de l'utilisateur. Chaque demande de modification d'un accès est formalisée et validée (cf. annexe «006.3 EDSR - Modele_recueil_utilisateurs »). La modification des accès est tracée à l'aide d'un système de journalisation.

c. Désactivation

Une désactivation d'un compte a lieu lors du départ d'un utilisateur ou d'un changement de mission. Chaque demande de désactivation d'un accès est formalisée et validée (cf. annexe «006.3 EDSR - Modele_recueil_utilisateurs »). La désactivation des accès est tracée à l'aide d'un système de journalisation.

d. Revues périodiques

Des revues de comptes sont menées régulièrement (a minima annuellement), afin de s'assurer que :

- les comptes administrateurs sont limités à un nombre restreint d'agents
- les utilisateurs actifs disposent d'accès strictement utiles à l'exercice de leurs missions et conformes à leur profil d'accès
- les utilisateurs actifs sont bien présents sur le site

Pour chaque revue réalisée, un rapport de contrôle indique :

- la date de la revue
- l'application dont les accès ont été révisés
- les actions correctives mises en œuvre
- l'identité du référent EDS ou de l'administrateur EDS de la DSI centrale qui a procédé à la revue

Les rapports de contrôle sont conservés a minima 18 mois par la direction du système d'information local.

e. Évaluations – Indicateurs

La DSI centrale s'assure de la bonne exécution des opérations de gestion des comptes pour les applications i2b2, Jupyter et Cohort360. Elle s'appuie sur les référents EDS de chaque GHU. Les demandes relatives à la gestion des accès sont conservées par l'équipe de l'EDS.

III. Matrice des habilitations

Des **profils d'accès** sont définis pour chaque application (i2b2, Jupyter, Cohort360). Les profils d'accès définissent les fonctionnalités accessibles aux utilisateurs.

a. i2b2

Tableau des profils d'accès :

Profils d'accès / Fonctionnalités		**i2b2 Console Admin**	**I2b2 Webclient**			
		ADMIN	OBFSC	AGG	LDS	**DEID**
ADMINISTRATION	Administration technique (hors exploitation)	☑	☑			
	Administration fonctionnelle	☑	☑			
UTILISATION	Déterminer un nombre de patients éligibles		☑	☑	☑	☑
	Nombre de requêtes limité		☑			
	Résultats masqués, approximatifs		☑			
	Nombre de requêtes illimité			☑	☑	☑
	Résultats exacts			☑	☑	☑
	Créer une liste pseudonymisée de patients (cohorte)			☑	☑	☑
	Analyser les données (plugins de base)				☑	☑
	Exporter les données des patients – pseudonymisé				☑	
	Exporter les données des patients - nominatif					☑

Les **profils d'accès** à l'application n'ont pas évolué depuis la demande d'autorisation initiale de l'EDS de l'AP-HP. Les profils existants sont donc toujours les suivants :

1. **OBFSC** : Profil d'accès à des données agrégées floutées

Un utilisateur possédant le profil « accès à des données agrégées floutées » (« OBFSC ») ne pourra réaliser qu'un nombre limité d'exécutions de requête (7 requêtes identiques consécutives) et accéder uniquement à des nombres de patients correspondant à des critères de sélection dont la valeur est approximative lorsque le nombre est petit. L'utilisateur n'a pas accès à la liste des patients et ne peut pas exporter de données.

2. **AGG :** Profil d'accès à des données agrégées

Un utilisateur possédant le profil « accès à des données agrégées » (« AGG ») pourra effectuer autant de requêtes que nécessaire dans le cadre de son activité, accéder au nombre exact de patients correspondant à des critères de sélection et visualiser les caractéristiques de cette population de patients. L'utilisateur n'a pas accès à la liste des patients et ne peut pas exporter de données.

3. **LDS** : Profil d'export de données avec faible risque de réidentification

Un utilisateur possédant le profil « export de données avec faible risque de réidentification » (« LDS ») pourra effectuer autant de requêtes que nécessaire dans le cadre de son activité, accéder au nombre exact de patients correspondant à des critères de sélection et visualiser les caractéristiques de cette population de patients et, le cas échéant, exporter les données d'intérêt de ces patients à faible risque de réidentification (exclusion de l'Identifiant Permanent Patient, du Numéro du Dossier Administratif, de la date de naissance, de la date de décès, du code postal de ville de naissance et des comptes rendus).

4. **DEID** : Profil d'export de données avec réidentification

Un utilisateur possédant le profil « export de données avec réidentification » (« DEID ») pourra effectuer autant de requêtes que nécessaire dans le cadre de son activité, accéder au nombre exact de patients correspondant à des critères de sélection et visualiser les caractéristiques de cette population de patients et, le cas échéant, exporter les données d'intérêt de ces patients y compris des données identifiantes.

b. JUPYTER

L'accès à Jupyter est réservé aux chercheurs (internes et externes à l'AP-HP) dont le projet a été autorisé par le Comité Scientifique et Ethique de l'EDS pour les recherches multicentriques. Le périmètre d'utilisation de Jupyter pourrait s'étendre aux recherches internes menées par les équipes de soins.

Un numéro est attribué pour chaque recherche par le secrétariat du CSE (règle de nommage : CSE-AA-nnnn / AA = Année ; nnnn = séquenceur).

Un espace de travail Jupyter privé et sécurisé et portant le numéro CSE attribué est ensuite créé sur la plateforme EDSR par l'administrateur DSI de l'EDS.

Les comptes utilisateurs Jupyter sont gérés directement dans l'Active Directory de l'AP-HP. L'administrateur DSI de l'EDS créé un groupe AD par projet CSE. Les utilisateurs de l'équipe de recherche sont ajoutés au groupe AD dédié.

L'utilisateur se connecte au portail Jupyter en renseignant son login (suffixe = Numéro de projet CSE + Code APH) et son mot de passe AD. L'authentification du compte se fait via l'AD.

L'utilisateur autorisé accède à l'espace de travail Jupyter dédié contenant les données strictement nécessaires à la recherche. Par défaut, les données ont fait l'objet d'une procédure de pseudonymisation décrites dans le PIA EDSR (profil d'accès **PSEUDO**). Dans les cas particuliers et sous réserve d'une autorisation de la CNIL, les données directement identifiantes peuvent être mise à disposition des chercheurs (profil d'accès **NOMI**). Par défaut, les données analysées ne peuvent pas être exportées.

A terme, une console d'administration des comptes utilisateurs Jupyter sera développée (profil d'accès **ADMIN**).

c. Cohort360

Dans sa version v1.1, Cohort360 permet de visualiser les données des patients sélectionnés dans i2b2. Les comptes utilisateurs sont importés depuis i2b2. Il faut donc avoir suivi la procédure d'accès à i2b2 pour avoir un compte Cohort360. Les données visibles dans Cohort360 sont actuellement des données nominatives. Un faible nombre de comptes ont pour l'instant été ouverts à des personnes prenant part au développement de Cohort360.

Les utilisateurs de Cohort360 ont accès aux données de l'EDS Recherche en lecture seule. A terme les fonctionnalités de Cohort360 seront regroupées en deux profils d'accès :

- Accès aux données nominatives (**NOMI**).

Le profil d'accès NOMI sera réservé aux personnels de l'équipe de soin (périmètre des données accessibles =celui des patients pris en charge par l'équipe de soin) et aux médecins DIM (périmètres GHU ou tout l'APHP, respectivement pour les médecins DIM du siège et ceux des GHU).

- Accès aux données pseudonymisées (**PSEUDO**).

Dans le profil d'accès PSEUDO, les données suivantes sont obfusquées : nom, prénom, Identifiant Permanent Patient, Numéro du Dossier Administratif, date de naissance, date de décès, code postal de ville de naissance). Le profil d'accès PSEUDO sera réservé aux chercheurs travaillant sur une cohorte de recherche (sur le périmètre du protocole) et aux personnels des URC et des unités de santé publique sur le périmètre de leurs fonctions pour le support méthodologique.

Une console d'administration des comptes utilisateurs Cohort360 est en cours de développement, dont l'accès est réservé aux profils d'accès administrateur. Les administrateurs centraux (**ADMINCENT**) peuvent définir les profils d'accès et les affectations sur tout le périmètre de l'APHP. Les administrateurs locaux (**ADMINLOC**) peuvent affecter des profils d'accès aux personnels de leur périmètre (GHU). L'application Cohort360 inclura de nouvelles fonctionnalités et de nouveaux profils d'accès par fonctionnalité pourront être définis à moyen terme.

La gestion des comptes utilisateurs se réalise dans le Back end de Cohort360 (base de données au format OMOP).

- Une table de Rôle définit la confidentialité des données. Elle comporte 4 rôles :
  - Rôle 1 : profil d'accès **NOMI**
  - Rôle 2 : profil d'accès **PSEUDO**
  - Rôle 3 : profil d'accès **ADMINCENT**
  - Rôle 4 : profil d'accès **ADMINLOC**
- Une table de sécurité Patient/Service définit quel patient a été pris en charge dans quel service (appartenance à une Equipe de soins)
- Une table d'affectation basée sur la structure hospitalière définit les comptes : un compte utilisateur (code APH) est associé à un rôle et à un niveau de la structure hospitalière.

Aperçu de l'annexe : « 006.2 EDSR - Matrice des habilitations »

EXTRAIT DE LA MATRICE D'HABILITATIONS

		1			4				
		Personnel d'une équipe de soin et assimilé			Personnel autorisé par un protocole d'étude (utilisateur final) = Equipe de recherche Ex : recherche multicentrique validée par le comité Scientifique et Ethique (CSE)				
		Personnel médical	Personnel paramédical	IRC - Ingénieur de recherche clinique (Chef de projet -	Personnel médical	Personnel paramédical	Equipe de recherche	Datascientist	Bio statisticien
Finalités	**Recherche interne** sur données dite "équipe de soins" (ex: Thèse de l'interne, Vérifier une hypothèse, ...)	✓	✓						
	Recherche multicentrique sur données dans le cadre d'un protocole autorisé (Ex : CSE)				✓	✓	✓	✓	✓
	Screening de patients dans le cadre d'études ou de registres pour la recherche clinique, c'est-à-dire, trouver les patients correspondant aux critères d'inclusion ou de non-inclusion (en vue de consultation des dossiers électroniques et/ou papiers pour saisie dans les e-CRF)			✓					
	Contrôle qualité pour une période donnée pour la recherche clinique								
	Récupération des données pour la recherche clinique								
	Etude de faisabilité	✓	✓						
	Recherche sur données dans le cadre des **missions du DIM**								
	Réalisation de traitements sur les données (cœur de métier DIM)								
	Création d'une liste de patients (cœur de métier DIM) pour lesquels il manque un code PMSI (Ex : existence du terme « sepsis » dans le CRH et pas de codage A40x ou A41)								
	Transmission des listes de patients aux TIM pour recodage des séjours								
Périmètre géographique - Population de patients	Périmètre " équipe de soins " : accès aux données des patients pris en charge au moins une fois dans l'UFR ou aux données des patients à qui un résultat est rendu (pour les plateaux médico techniques, les services d'anatomie pathologiques, la pharmacie)	✓	✓	✓					
	Périmètre " multicentrique " restreinte aux données des patients éligibles en fonction des critères d'inclusion et de non inclusion d'un protocole autorisé (Ex : CSE)				✓	✓	✓	✓	✓
	Périmètre " AP-HP - Etude faisabilité" : accès aux données des patients de l'AP-HP								
	Périmètre " GHU " : accès aux données des patients pris en charge au moins une fois au sein du GH								
	Périmètre " AP-HP - DIM " : accès aux données des patients de l'AP-HP dans le cas de leur mission								
	Périmètre " GHU - Support " dans le cadre du support informatique								
	Périmètre " AP-HP - Support " dans le cadre du support informatique								
Nature et périmètre des données	L'ensemble des données des patients contenues dans l'EDS (couvert par l'autorisation CNIL), strictement nécessaires à la recherche, quel que soit le site de collecte de ces données lors du parcours des patients à l'AP-HP	✓	✓	✓	✓	✓	✓	✓	✓
Profil d'accès par défaut	i2b2 : Requête sur « Données agrégées floutées » (« OBFSC »), sans export de données								
	i2b2 : Requête sur « Données agrégées » (« AGG »), sans export de données				✓	✓	✓	✓	✓
	i2b2 : Export de données avec faible risque de réidentification (« LDS »)								
	i2b2 : Export de données identifiantes ("DEID")	✓	✓	✓					
	i2b2 : ADMIN								
	Cohort360 : NOMI	✓	✓	✓					
	Cohort360 : PSEUDO				✓	✓	✓	✓	✓
	Cohort360 : ADMINCENT								
	Cohort360 : ADMINLOC								
	Jupyter : NOMI	✓	✓	✓					
	Jupyter : PSEUDO				✓	✓	✓	✓	✓
	Jupyter : ADMIN								
Profil attribué par :	Le reponsable hiérarchique de l'utilisateur	✓	✓	✓					
	Le responsable des données défini dans le protocole d'étude				✓	✓	✓	✓	✓