



MY HEALTH MY DATA, UN MODÈLE OPÉRATIONNEL

Auteur : EFCSE, Working Group Blockchain
26 février 2020

Présentation du pilote

Le 26 février 2020 a eu lieu, devant des représentants de la Commission Européenne (revue finale), la présentation du pilote européen de MHMD par l'équipe projet et le plan de déploiement du prototype dans les établissements de soins et de recherche.

LE PILOTE CONCERNE 80 000 PATIENTS,
820 000 EVENEMENTS MEDICAUX ET
71 MILLIONS DE DONNEES DE SANTE (VARIABLES CLINIQUES).

Le système permet le transfert de données entre différents partenaires sur des lieux géographiques distincts en Europe.

Les données sont stockées dans ces 4 hôpitaux européens qui jouent le rôle de contrôleurs des informations

- Queen Mary University of London [QMLU] – EN
- Ospedale Pediatrico Bambino Gesù [OPBG] – IT
- CHU Hôpital de la CHARITE – FR
- Centre hospitalier - Université Catholique de Louvain [UCL]- BE

Le traitement des données est effectué par 2 sociétés spécialisées dans ce domaine : GNUBILA / be-ys Group et Siemens.

A propos de My Health My Data (MHMD),

MHMD est une action de recherche et d'innovation du programme de l'Union Européenne Horizon 2020, visant à changer fondamentalement la façon de partager les données sensibles.

MHMD est en passe d'être le premier réseau d'information biomédicale ouvert centré sur la connexion entre les organisations et les individus, encourageant les hôpitaux à commencer à mettre des données anonymisées à la disposition de la recherche ouverte, tout en incitant les citoyens à devenir les propriétaires et contrôleurs ultimes de leurs données de santé.

MHMD est destiné à devenir un véritable marché de l'information, basé sur de nouveaux mécanismes de confiance, de relations directes et basées sur la valeur entre les citoyens de l'UE, les hôpitaux, les centres de recherche et les entreprises.

Rappel des principaux objectifs de MHMD

- Utiliser la technologie BLOCKCHAIN pour permettre aux données personnelles, y compris médicales, d'être stockées et transmises de manière sûre et efficace dans un espace européen dédié,
- Intégrer toutes les technologies de protection et préservation d'identité et de confidentialité,
- Développer une interface de consentement dynamique pour les personnes dans la gestion des accès à leurs données en fonction de différents types d'utilisation,
- Utiliser des contrats intelligents (SMART CONTRAT) pour aider les personnes concernées dans leur droit d'accès, d'effacement, de modification, de suppression de leurs informations allant jusqu'au droit à l'oubli (application du RGPD).



La présentation à la Commission Européenne a fait la démonstration de la blockchain dans un modèle de respect de l'anonymat, ceci est une 1^{ère} car jusqu'à présent, il a toujours été souligné cette incompatibilité entre technologie blockchain et respect de la protection des données personnelles, donc de l'application du RGPD.

Sur le principe, le registre des échanges de données est anonyme mais toute loi de type RGPD est applicable et peut être traduite en smart contrat par la blockchain, ainsi, par conception, c'est du Privacy by Design.

Le système présenté intègre :

- PSEUDONYMISATION (traitement des données personnelles afin qu'on ne puisse pas les attribuer à une personne physique sans disposer d'informations supplémentaires),
- ANONYMISATION (technique permettant de contrecarrer l'identification d'une donnée de façon irréversible),
- CONFIDENTIALITE DIFFERENTIELLE (mécanismes de génération aléatoire de « bruits », à savoir, création d'information synthétiques supplémentaires en vue d'augmenter la probabilité statistique des groupes discriminants afin d'empêcher de remonter au groupe réel initial),
- SECURE MULTI-PARTY COMPUTATION (domaine cryptographique/ calcul à préservation de confidentialité)
- CHIFFREMENT HOMOMORPHIQUE (domaine cryptographique/ manipulation des données chiffrées sans nécessité de les déchiffrer)

Lors de cette présentation il a été fait démonstration de 2 cas d'usage :

- Cas d'utilisation institutionnel : données pour la recherche [enregistrement, téléchargement et calcul sécurisé]
- Cas d'utilisation individuel : inscription, téléchargement et droit à l'oubli [intégration de 2 applications mobiles pour les données de santé et les données personnelles en provenance des réseaux sociaux]

SOULIGNONS QU'IL A ETE FAIT LA DEMONSTRATION CONCRETE DU RESPECT DU DROIT A L'OUBLI OU DROIT A L'EFFACEMENT (ARTICLE 17 DU RGPD).

Les prochaines étapes

MHDM fait l'objet d'un transfert vers l'industrie avec une première version industrielle, PROREGISTER prévue :

- En Juin 2020 sous forme d'un PMV¹ avec gestion des logs sur la blockchain.
- En Septembre 2020 avec un PMV intégrant tous les droits RGPD.

Cette extension est prévue avec les partenaires de l'Openlab du CERN, qui s'inscrit dans le cadre de la collaboration du groupe be-ys, portée par David MANSET CEO & co-Founder be-studys, avec le CERN.

A terme, cette plateforme, qui a bénéficié de 3,5 millions d'euros de financement de la Commission européenne ambitieuse, notamment, d'être un outil capable de relier les différentes plateformes nationales de donnée en Europe, telle que le Health Data Hub français.

¹ PMV : produit minimum viable



FOCUS SUR LE PRINCIPE DE CONFORMITE DE LA BLOCKCHAIN AVEC LE RGPD

1 - DONNEES

- Stockage privé de données hors de la blockchain (via FedEHR* Data Capsule & Driver).
- Enregistrement anonyme dans la blockchain des informations sur l'état du processus de partage de données.

A propos de FedEHR

- Référentiel de dossier de santé électronique hautement sécurisé, indépendant du fournisseur et centré sur la personne
- Permet une intégration hétérogène de données médicales à partir de différents emplacements physiques (géographiques)
- Offre une vue unique et intégrée des données
- Apporte une puissance de navigation et d'analyse des données

2 – CONSENTEMENT DYNAMIQUE

- Prise de contrôle sur ses propres données (qui y a accès et dans quel but ?)
- Requise par l'application mobile MHMD, associée à un contrat intelligent et un RTBF* exécutable.

3- PROTECTION DE L'IDENTITE ET DES DROITS DU PROPRIETAIRES DES DONNEES

- Différents niveaux de pseudo-anonymisation.
- Système de blockchain préservant la confidentialité (empêchant l'inférence statistique).
- Droit à l'oubli, un contrat intelligent supprime le lien entre la blockchain et les données hors chaîne.

4 – BLOCKCHAIN ET CONTRAT INTELLIGENT

- Contrats intelligents pour orchestrer le cycle de vie du partage de données, appliquer les politiques de sécurité (et exécution des droit RGPD) et les différentes règles métier.
- Conservation de la trace de toutes les actions réalisées dans le système pour le processus de partage de données.
- Conception modulaire permettant d'utiliser différents types d'algorithmes de consensus, c'est-à-dire le mécanisme suivant lequel un réseau blockchain atteint un consensus (par exemple, ZKP² ou PBFT³).

[Plus d'information ?](#)

[Contactez-nous via notre site EFCSE.](#)

² Zéro Knowledge Proof: protocole de partage de données numériques entre 2 parties sans utilisation de mot de passe ou d'informations associées à la transaction.

³ Tolérance aux fautes Byzantines en pratique, concerne la remise en cause de la fiabilité des transmissions et de l'intégrité des interlocuteurs.