Deutsche Version (siehe unten)
Version française (ci-dessous)

Lay Summary

Project title	MedCo: Enabling the Secure and Privacy-Preserving Exploration of Distributed Clinical and *Omics Cohorts in the Swiss Personalized Health Network
Main applicant	SPHN: Nicolas Rosat, Direction of Information Systems, Lausanne University Hospital (CHUV) PHRT: Prof. Jean-Pierre Hubaux, School of Computer and Communication Sciences, École Polytechnique Fédérale de Lausanne (EPFL)
Consortium	EPFL, CHUV, HUGs, Insel
Short Summary	MedCo (https://medco.epfl.ch/) is the first operational system that makes sensitive medical data available for research in a simple, private and secure way. MedCo enables researchers to search for individuals that correspond to given clinical and genetic criteria all the while preserving individuals' privacy with strong end-to-end homomorphic encryption. MedCo has been co-developed by EPFL and CHUV and this infrastructure development project focuses at bringing MedCo from its current academic prototype version to a production-ready and hospital-compliant version in order to be deployed and used in the Swiss Personalized Health Network.
Background	The increasing number of health-data breaches is creating a complicated environment for medical-data sharing and, consequently, for medical progress. Therefore, the development of new solutions that can reassure clinical sites by enabling privacy-preserving sharing of sensitive medical data in compliance with stringent regulations (e.g., HIPAA, GDPR) is now more urgent than ever. To address this issue, EPFL and CHUV have jointly developed the first prototype of MedCo, an open-source privacy-preserving distributed system that integrates current cohort explorers and provides strong security and privacy guarantees such as trust decentralization, end-to-end data protection, auditability and differential privacy. To achieve these guarantees, MedCo relies on sophisticated privacy-enhancing technologies such as secure multi-party computation, homomorphic encryption and result obfuscation. So far, MedCo has been tested on a simulated and controlled academic environment. Results show impressive performance. The query runtime is comparable to the ones of state-of-the-art cohort explorers (e.g., i2b2) that do not provide any protection guarantees besides basic access control.
Goal	Despite its great potential, the current version of the MedCo prototype is still immature for being deployed and used in an operational clinical environment at Swiss hospitals. The goal of this project is very practical: bringing MedCo from its current academic prototype version into a

	production-ready version to be deployed and used in the Swiss Personalized Health Network.
Significance	The proposed project addresses a main challenge to further develop personalized health research, namely providing a mechanism to share sensitive and identifying health data (e.g., *omics data) across several medical institutions in a totally privacy-preserving and secure way. To ease its adoption at clinical sites, MedCo supports the APIs and data models of the i2b2 (Informatics for Integrating Biology and Bedside) framework and features an intuitive and modern user interface. Hospitals that already use i2b2 or similar tools can easily deploy MedCo on top of their existing infrastructure.

Deutsch

Projekttitel	MedCo: Befähigung zur sicheren und datenschutzwahrenden Erforschung dezentralisierter klinischer und *omics-Kohorten im Swiss Personalized Health Network (SPHN)
Hauptgesuchsteller	SPHN: Nicolas Rosat, Direction of Information Systems, Lausanne University Hospital (CHUV) PHRT: Prof. Jean-Pierre Hubaux, School of Computer and Communication Sciences, École Polytechnique Fédérale de Lausanne (EPFL)
Konsortium	EPFL, CHUV, HUGs, Insel
Kurzzusammen-fassung	MedCo (https://medco.epfl.ch/) ist das erste Betriebssystem, das sensible medizinische Daten für die Forschung auf einfache, vertrauliche und sichere Weise zur Verfügung stellt. MedCo ermöglicht es Forschern, nach Individuen zu suchen, die spezifischen klinischen und genetischen Kriterien entsprechen, und dabei gleichzeitig die Privatsphäre des Einzelnen dank einer starken End-to-End homomorphen Verschlüsselung zu schützen. MedCo wurde von EPFL und CHUV gemeinsam entwickelt. Das vorliegende Projekt hat zum Ziel, MedCo von seiner aktuellen akademischen Prototypversion in eine produktionsreife und spitalkonforme Version zu überführen, damit es schliesslich im SPHN-Netzwerk eingesetzt und genutzt werden kann.
Hintergrund	Die zunehmende Zahl von Verstössen im Bereich der Gesundheitsdaten schafft ein kompliziertes Umfeld für den Austausch medizinischer Daten und damit für den medizinischen Fortschritt. Die Entwicklung neuer Lösungen ist heute deshalb dringender denn je. Klinische Standorte sollen erneut Vertrauen gewinnen, indem der vertrauliche Austausch sensibler medizinischer Daten unter Einhaltung strenger Vorschriften (z.B. HIPAA, GDPR) ermöglicht wird. Um dieses Problem anzugehen, haben die EPFL und CHUV gemeinsam einen ersten Prototyp von MedCo entwickelt. MedCo ist ein Open-Source basiertes, dezentralisiertes System, welches Datenschutz gewährt und aktuelle Kohorten Explorer integriert. MedCo bietet robuste Sicherheits- und Datenschutzgarantien, wie beispielsweise Vertrauensdezentralisierung, durchgehenden Datenschutz, Überprüfbarkeit und differentielle Privatsphäre. Um diese Garantien zu erreichen, greift MedCo auf hochentwickelte, die Privatsphäre schützende Technologien zurück. Dazu gehören sichere verteilte Berechnungen, homomorphe Verschlüsselung und Ergebnisverschleierung. Bisher wurde MedCo in einer simulierten und kontrollierten akademischen Umgebung getestet. Die Ergebnisse sind vielversprechend und zeigen eine beeindruckende Leistung. Die Query-Laufzeit ist vergleichbar mit jener von modernen Kohorten Explorern (z.B. i2b2), die abgesehen von einer einfachen Zugangskontrolle keine Schutzgarantien bieten.
Ziel	Trotz seines grossen Potenzials ist die aktuelle Version des MedCo-Prototyps für den Einsatz und die Nutzung in einer klinischen

	Betriebsumgebung an Schweizer Spitälern noch nicht ausgereift. Das Ziel dieses Projekts ist sehr praxisnah: MedCo soll von seiner aktuellen akademischen Prototypversion in eine produktionsreife Version gebracht werden, die im SPHN Netzwerk eingesetzt und genutzt werden kann.
Bedeutung	Das vorgeschlagene Projekt widmet sich der grossen Herausforderung, die Forschung im Bereich der personalisierten Gesundheit voranzutreiben. Und zwar soll ein Mechanismus entwickelt werden, welcher den Austausch sensibler und identifizierender Gesundheitsdaten (z.B. *omics-Daten) auf sichere und Privatsphäre bewahrende Weise zwischen mehreren medizinischen Einrichtungen ermöglicht. Um die Akzeptanz an klinischen Standorten zu erleichtern, unterstützt MedCo die APIs und Datenmodelle des i2b2 (Informatics for Integrating Biology and Bedside) Systems und verfügt über eine intuitive und moderne Benutzeroberfläche. Spitäler, die bereits i2b2 oder ähnliche Tools verwenden, können MedCo problemlos zusätzlich zur bestehenden Infrastruktur einsetzen.

Français

Titre du projet	MedCo : Permettre l'exploration sécurisée et respectueuse de la vie privée de données cliniques et *omiques distribuées dans le Swiss Personalized Health Network
Requérant principal	SPHN: Nicolas Rosat, Direction of Information Systems, Lausanne University Hospital (CHUV) PHRT: Prof. Jean-Pierre Hubaux, School of Computer and Communication Sciences, École Polytechnique Fédérale de Lausanne (EPFL)
Consortium	EPFL, CHUV, HUGs, Insel
Résumé	MedCo (https://medco.epfl.ch/) est le premier système opérationnel qui met à disposition des données médicales sensibles pour la recherche de manière simple, privée et sécurisée. MedCo permet aux chercheurs de rechercher des individus qui correspondent à des critères cliniques et génétiques précis tout en préservant la vie privée des individus grâce au cryptage homomorphe. MedCo a été co-développé par l'EPFL et le CHUV et ce projet de développement d'infrastructure vise à faire évoluer MedCo de sa version de prototype académique actuelle à une version adaptée à un environnent de production dans les hôpitaux afin de la déployer et l'utiliser dans le contexte du Swiss Personalized Health Network.
Contexte	Le nombre croissant d'atteintes à la protection des données relatives à la santé crée un environnement complexe pour le partage des données médicales et, par conséquent, pour le progrès médical. Ainsi, le développement de nouvelles solutions permettant de sécuriser les établissements cliniques en permettant le partage de données médicales sensibles dans le respect de la vie privée conformément à des réglementations strictes (HIPAA, GDPR) est plus urgent que jamais. Pour résoudre ce problème, l'EPFL et le CHUV ont développé conjointement le premier prototype de MedCo, un système distribué open-source de protection de la vie privée qui intègre les explorateurs de cohortes actuels et offre de solides garanties de sécurité et de confidentialité telles que la décentralisation de la confiance, la protection de bout en bout des données, l'auditabilité et la confidentialité différentielle. Pour obtenir ces garanties, MedCo s'appuie sur des technologies sophistiquées d'amélioration de la protection de la vie privée telles que le secure multi-party computation, le cryptage homomorphe et l'obscurcissement des résultats. Jusqu'à présent, MedCo a été testé dans un environnement académique simulé et contrôlé. Les résultats sont impressionnants. La durée d'exécution de la requête est comparable à celle des explorateurs de cohortes de pointe (p. ex., i2b2) qui n'offrent aucune garantie de protection en plus du contrôle d'accès de base.
But	Malgré son grand potentiel, la version actuelle du prototype MedCo n'est pas encore mûre pour être déployée et utilisée dans un environnement

	clinique opérationnel dans les hôpitaux suisses. L'objectif de ce projet est très pratique : faire passer MedCo de sa version prototype académique actuelle à une version prête à la production qui sera déployée et utilisée dans le Swiss Personalized Health Network.
Importance	Le projet proposé s'attaque à l'un des principaux défis du développement de la recherche personnalisée en santé : savoir fournir un mécanisme de partage de données de santé sensibles et identifiantes (p. ex., données *omiques) entre plusieurs établissements médicaux, d'une manière totalement sécurisée et préservant la vie privée des intéressés. Pour faciliter son adoption dans les hôpitaux, MedCo supporte les API et les modèles de données du système i2b2 (Informatics for Integrating Biology and Bedside) et offre une interface utilisateur intuitive et moderne. Les hôpitaux qui utilisent déjà i2b2 ou des outils similaires peuvent facilement déployer MedCo en plus de leur infrastructure existante.