

La ricerca Europea sulle nuove tecnologie per la privacy. Il dato sanitario diventa strumento di sostenibilità per il Servizio Sanitario.

Background

L'uso secondario del dato di salute rimane per lo più un'opportunità non realizzata ^{1,2}, fra l'altro, per i limiti imposti dalla protezione della privacy. La frizione intrinseca fra uso del dato e riservatezza, però, è stata oggetto di intensi programmi di ricerca con l'entrata in vigore del GDPR portando a perfezionare tecnologie che oggi consentono di proteggere dati sensibili e al contempo di riusarli in scala. Questo studio presenta una piattaforma finanziata da progetti Horizon 2020 (MyHealth-MyData [ID: 732907], euCanShare [ID: 825903], Kraken [ID: 871473]), per facilitare lo scambio sicuro ed efficiente di dati sanitari senza rischi etico legali e accelerandone la valorizzazione da parte dei servizi sanitari che trovano così un nuovo strumento per sostenere finanziariamente il proprio sviluppo e la ricerca clinica.

Metodi

La piattaforma ha integrato:

1. Una Blockchain su cui soggetti e Titolari specificano il proprio consenso e che nel contempo fornisce un registro immutabile e verificabile di tutti gli accessi.
2. Un sistemi di Secure Multi-Party Computation (SMPC) che consente a terzi di eseguire analisi, mantenendo localmente criptati i dati di ciascun partecipante, facilitando la ricerca senza condivisione diretta dei dati.
3. La Privacy Differenziale che introduce rumore controllato assicurando che i dati individuali siano offuscati, ma le query aggregate restino utili.

Il design è stato iterativo, incorporando feedback da ricercatori, professionisti sanitari e gruppi di pazienti.

Risultati

La piattaforma è oggi in uso, nel progetto EBRAINS e DataTools4Heart, in più di 20 centri accademici europei che la utilizzano a fini di ricerca e sviluppo d'intelligenza artificiale.

Tramite SMPC, ricercatori hanno ad oggi analizzato più di 100 dataset cardiologici e di neuroscienze senza accedere direttamente a dati sensibili.

La blockchain ha aumentato la trasparenza e la fiducia, come misurato con questionari personalizzati, tra i 52 pazienti arruolati che hanno condiviso dati.

Le analisi protette con privacy differenziale, si sono dimostrate resistenti ad attacchi inferenziali di re-identificazione in 2 test di laboratorio.

Conclusioni

¹ Gerlinger, C., Evers, T., Rassen, J. et al. Using Real-World Data to Predict Clinical and Economic Benefits of a Future Drug Based on its Target Product Profile. *Drugs - Real World Outcomes* 7, 221–227 (2020). <https://doi.org/10.1007/s40801-020-00203-w>

² Uwizeyemungu S, Poba-Nzaou P, Cantinotti M. European Hospitals' Transition Toward Fully Electronic-Based Systems: Do Information Technology Security and Privacy Practices Follow? *JMIR Med Inform*. 2019 Mar 25;7(1):e11211. doi: 10.2196/11211. PMID: 30907732; PMCID: PMC6452275.

La Commissione Europea stima che un uso in scala del dato clinico possa far risparmiare 11 miliardi di euro in 10 anni³ ai sistemi sanitari del Continente. Ernst and Young ne stima il valore, per il solo NHS Inglese, a circa 9 miliardi di sterline all'anno⁴.

La combinazione di blockchain, SMPC e privacy differenziale garantisce che privacy e utilità dei dati non siano più mutuamente esclusive, consentendo collaborazioni transfrontaliere e fra attori pubblici e privati. Questo realizza un nuovo paradigma in cui ospedali e pazienti possono definire chi può accedere alle proprie informazioni, per quale uso, per quanto tempo, e a quale costo, mentre i dati vengono interrogati in analisi distribuite sotto garanzie matematiche di anomia dei risultati. Il complesso integrato di queste tecnologie, in altre parole, disaccoppia le informazioni sensibili dalle inferenze statistiche e rende possibile la valorizzazione diretta dell'informazione anonima conservata nei sistemi sanitari fornendo a questi un nuovo strumento di sostenibilità e crescita.

³ [Salute dell'UE: spazio europeo dei dati sanitari \(europa.eu\)](https://ec.europa.eu/health/eu_data_space_en)

⁴ [ey-value-of-health-care-data-v20-final.pdf](#)