Public Health and Informatics
J. Mantas et al. (Eds.)

doi:10.3233/SHTI210212

Clientside Pseudonymization with Trusted Third-Party Using Modern Web Technology

Adam MAHMOUD[a,1], Bernd AHLBORN[a],
Ulrich MANSMANN[a] and Isabel REINHARDT[a,b]
[a] *Institute for medical Information Processing, Biometry and Epidemiology, Ludwig-Maximilians-Universität München, Munich, Germany*
[b] *Trusted Third Party of the Faculty of Medicine, Ludwig-Maximilians-Universität München, Munich, Germany*

Abstract. There is a demand for a pseudonymization service by a Trusted Third Party (TTP), that features clientside pseudonymization. We propose a system using modern web technology, which requires no installation but can handle data preprocessing and pseudonymization safely on the client.

Keywords. data security, privacy protection, data pseudonymization, trusted third party, secondary use

1. Introduction

More and more clinical institutions start to organize their data in digital patient records and increasingly make these data available for secondary use in medical research. Pseudonymization standards for clinical research aim to protect privacy of the individuals involved [1-6]. We present a trusted-third-party (TTP) concept that uses modern web technology to enable pseudonymization and privacy-preserving record linkage, without on-site installation and still realizes the security that can be achieved by double pseudonymization. In comparison, existing solutions either offer no pre-processing on the client or require the local installation of software [3,5,6].

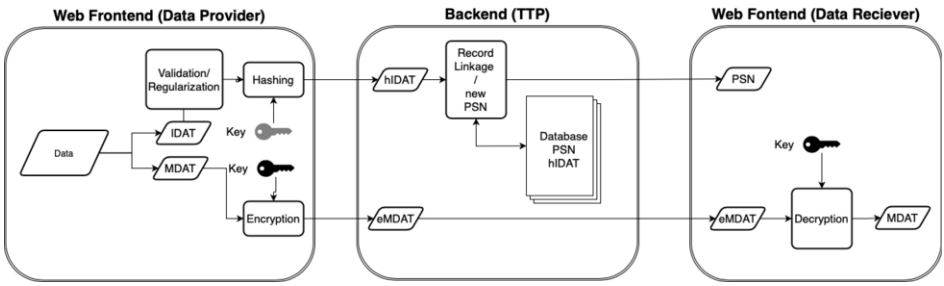

Figure 1. Dataflow Diagram for the clientside Pseudonymization service.

[1] Corresponding Author, Adam Mahmoud, Institute for medical Information Processing, Biometry and Epidemiology, Marchioninistr. 15; 81377 Munich, Germany; E-mail: adam.mahmoud@ibe.med.uni-muenchen.de.

2. Methods

We defined the following requirements based on existing concepts: privacy-preserving, high data protection level, user friendly, configurable. We implemented a prototype using modern web technology. In the process the MDAT is encrypted (eMDAT) with a key that is known to all parties involved except the TTP. The IDAT is hashed (hIDAT) with a key only known to the data provider. The record linkage of hIDAT was tested in a search for patients treated in several centers for the same disease.

3. Results

The researcher hands the data to the TTP via a web-frontend. The frontend performs a data-validation, -regularizations, hashing of the IDAT and encryption of the MDAT. It is sent to the remote backend (TTP), where a unique set of hIDAT is processed as follows: If the set matches an existing one, the corresponding pseudonym (PSN) is assigned. Otherwise, a new PSN is generated. The data receiver gets the PSN and the eMDATs via the frontend. The eMDAT is decrypted on-premise by providing the key.

4. Discussion

Although IDAT, as well as MDAT, is passed over through the TTP, informational separation of powers is held in place due to encryption. As the front-end is built in JavaScript, no on-site installation is required.

5. Conclusion

The presented concept and pilot show that data transfer, privacy preserving record linkage and pseudonymization can be performed on a web application hosted by a TTP.

References

[1] Aamot HA, Kohl CH, Richter DA, Knaup-Gregori PE. Pseudonymization of patient identifiers for translational research. BMC Med Inform Decis Mak. 2013;13(1).
[2] Claerhout B, Demoor. G J E Privacy protection for clinical and genomic data. the use of privacy-enhancing techniques in medicine. Int J Med Inform. 2005;74(2–4).
[3] Bahls TO, Pung JO, Heinemann ST, Hauswaldt JO, Demmer IR, Blu-mentritt AR, et al. Designing and piloting a generic research architecture and workflows to unlock germanprimary care data for secondary use. J Transl Med. 2020;18(1).
[4] Bialke MA, Penndorf PE, Wegner TI, Bahls TO, Havemann CH, Piegsa JE, et al. A workflow-driven approach to integrate generic software modules in a trusted thirdparty. J Transl Med. 2015;13(1).
[5] Iheanyi Nwankwo EN. Providing a Network of Trust in Processing Health Data for Research [Internet]. 2014 Nov 18. Available from: https://silo.tips/download/providing-a-network-of-trust-in-processing-health-data-for-research
[6] 6. Godau J. sVst Schütze Vertrauensstelle [Internet]. 2018 [cited 2021 Mar 2]. Available from: https://www.tmf-ev.de/DesktopModules/Bring2mind/DMX/Download.aspx?Method=attachment&Command=Core_Download&EntryId=31690&PortalId=0