# Blockchain as an Enabler for Cybersecurity Use Case: Electronic Health Records in Switzerland

Pascal Moriggl[1], Petra Maria Asprion[1], Fabienne Kramer[1]

FHNW, University of Applied Sciences and Arts Northwestern Switzerland, CH-4002 Basel

**Abstract.** In the application of Electronic Health Records (EHR), cybersecurity is an essential control and needs to be strongly considered to fulfil data protection requirements. Regarding cybersecurity needs in Healthcare, blockchain-based technologies seem promising due to the inherent security features. Therefore, this study investigates in cybersecurity requirements for EHR and whether a blockchain-based solution can cover these. There are already approaches which apply Blockchain for EHR, but these do not explicitly consider cybersecurity, which forms the research gap. As a unit of analysis, 'Hyperledger Sawtooth' as an enterprise blockchain platform was used. The results showed that Hyperledger Sawtooth performs quite well regarding the coverage of cybersecurity-relevant requirements for EHR. However, there are 'natural' divergences concerning specific cybersecurity attributes between blockchain-based and non-blockchain-based systems. The outcome of this study is a generic assessment tool which can be used to assess the coverage of cybersecurity requirements for both blockchain-based and non-blockchain-based EHR systems.

**Keywords:** Hyperledger Sawtooth, Blockchain, Cybersecurity, Healthcare, Electronic Health Records.

## 1 Introduction

The rise of the Blockchain technology (in this study referred to as Blockchain) started back in the year 2008 with the publication of the whitepaper' Bitcoin: A Peer-to-Peer Electronic Cash System', that was published with the alias Satoshi Nakamoto [1]. Blockchain is, therefore, more than a decade around. Since the publication of the whitepaper, many other possible applications for Blockchain outside of cryptocurrencies emerged [2]. Gartner [3] lists in their 2018 hype cycle for emerging technologies' Blockchain for data security' - which is part of this study's focus area - in the innovation trigger phase and that it will reach the plateau in five to ten years. Blockchain itself is already descending on the cycle. However, Blockchain is still within the peak of the inflated expectations phase, which means that early publicity produces success stories but also failures [4]. While still in the early stages, there exist already some promising use cases regarding blockchain focused on cybersecurity applications [5] [6] [7].

Hölbl, Kompara, Kamišalić, & Zlatolas [8] argue that the Blockchain offers excellent potential for its use in Healthcare because this sector processes masses of sensitive

data for which data security must be guaranteed. Rabah [9] complement that Blockchain in Healthcare offers lower costs by, e.g., reducing waiting times, paperwork or avoiding multiple registration processes. Furthermore, Blockchain has unique characteristics that enable innovations in cybersecurity [7]. Cybersecurity is an essential need when establishing EHR because of the necessary adherence to regulations, mainly digital data protection. For this reason, this study addresses Blockchain as innovation and an enabler for cybersecurity in the context of Healthcare.

## 2 Research Rationales

This study evaluates the characteristics of Blockchain in the context of Healthcare in short 'health' and notably in the Swiss landscape, as a cybersecurity risk mitigation technology. Cyber threats are increasing and becoming steadily more targeted, complex and sophisticated. Especially the Healthcare sector is vulnerable to cyber threats. Healthcare organizations have with 6.45 million US Dollars the highest cost associated with data breaches for the ninth consecutive year. That is over 60% above the global average for all industries and therefore, more than the costs of a data breach in the financial sector [10]. Blockchain is extremely interesting for this sector because it offers promising opportunities to enhance cybersecurity [5,6,7]. According to Gartner [3], Blockchain 'has the potential to increase resilience, reliability, transparency and trust in centralized systems. This study aims at exploring whether a Blockchain can be used to enable cybersecurity for EHR in the first place. The following research questions were derived:

**RQ1:** What are the relevant cybersecurity-requirements for EHR?

**RQ2:** Hyperledger Sawtooth covers which requirements (RQ1)?

**RQ3:** How does Hyperledger Sawtooth compare to a 'traditional' data-based solution in terms of meeting the requirements (RQ2)?

EHR integrates an individual's medical health records generated by a health service provider (e.g. a physician, a medical assistant, a pharmacist) and private health records generated by the individual. EHR allows the sharing of data between authorized providers. However, an individual should be able to decide and provide its authorization [11]. This also applies to the situation in Switzerland where collections of personal documents with information about an individual's health will be stored in a nationwide system called 'Elektronisches Patientendossier'1, or 'Swiss Electronic Patient File' (EPF). It is aimed that this information can be accessed by the individual and authorized Healthcare providers at any time; the individual decides on who can view which information during which time frame [12]. The Swiss office of the national coordinator for 'Health Information Technology' [13] distinguishes between 'Electronic Medical Records' (EMR), 'Electronic Health Records' (EHR) and 'Personal Health Records' (PHR). EMR holds information that is created and located within a single Healthcare institution

[1] https://www.patientendossier.ch/de/bevoelkerung/kurz-erklaert (in German only)

(e.g. a medical centre or hospital). EHR, on the other hand, include information that can be managed, supplemented and accessed across several Healthcare institutions. Finally, PHRs are digital applications that enable an individual to access, manage and share the individual health information and that of others for whom he or she is authorized, in a private, safe and confidential environment. The Swiss EPF system will be such a digital PHR application that handles EHR. Health records are particularly sensitive data and underlie laws and regulations.

**Table 1.** Data types of PHR based on Roehrs et al. [17]

| Data Type | Reference |
|---|---|
| Allergies | Allergies and adverse reactions |
| Demographic | Patient statistics and clinical data |
| Documents | Attached files (photos, scanned documents) |
| Evolution | Progress and clinic notes, care plan |
| Family history | Family medical history |
| General | Patient registration information, emergency contact |
| Genetic | Genetic information |
| Home monitor | Home-monitored data |
| Immunizations | Immunization records (vaccine), tracking immunizations |
| Insurance | Insurance plan information, coding for billing |
| Laboratory results | Laboratory and imaging test results (laboratory tests) |
| Major illnesses | List of major diseases |
| Medications | Medication list prescribed, past medicines taken |
| Prescriptions | Medical prescription refills (renewing) |
| Prevention | Preventive health recommendations |
| Providers | Previous Healthcare provider list |
| Scheduling | Appointments, past procedures, hospitalizations |
| Social history | Social history, lifestyle (health habits) |
| Summaries | Admissions, permanency, and discharges |
| Vital signs | Status of bodily functions |

According to the Swiss Federal Act on Data Protection (DSG) Art. 3 para. c dig. 2 health, intimacy or racial origin are particularly sensitive personal data. These data may only be processed with the explicit permission of the person concerned (DSG Art. 4 para. 5). As a total revision of the Swiss DSG is being planned [14], the current legal situation in the European Union (EU) with its relatively new 'General Data Protection

Regulation' (GDPR) is sketched out below. GDPR came into effect in 2018 and affected subjects (citizens or residents of the EU) as well as controllers (persons who determine how and why personal data is processed) and processors (third parties who process personal data for a data controller). GDPR is one of the world's strictest data protection and security law. Violating fines are at a maximum of 20 million Euro or 4% of the global revenue [15]. Based on GDPR, it is forbidden to process health data unless exceptions apply. One of the exceptions is when the subject gives explicit consent to the processing (GDPR Art. 9). In practice, several different EHR data types on an individual's level (PHR) can occur in a digital application and are subject to the law, such as stated in the GDPR description. Roehrs, Da Costa, Da Rosa Righi, & De Oliveira [17] derived from 48 articles a list of datatypes used in PHR applications such as the Swiss EPF is. It can be anticipated that EHR may include all or particular data types listed in Table 1. In contrast to the data types in Table 1, EHRs also contain additional information outside of the medical field, such as access logs, access, change rights or service provider information.

An assessment tool could provide a point of reference for digital EHR systems to comply with legal (e.g. GDPR) and technical (e.g. cybersecurity) requirements in Healthcare. Therefore, the next section is dedicated to the compilation of cybersecurity requirements/criteria that such systems ideally should fulfil.

## 3 Cybersecurity Requirements for EHR

Hoerbst & Ammenwerth [18] published a highly regarded study in which they compiled an extensive list of qualitative requirements for EHR systems. They collected criteria that relate to cybersecurity attributes such as 'confidentiality', 'integrity', 'availability', 'authenticity' or 'data security' [19].

The (cyber) security-related attributes are explained in the following: 'confidentiality' is given if the data in a system is only accessible to authorized persons. Measures must be taken to ensure access rights and access protection [20] and to guarantee confidentiality. 'Integrity' may include authenticity and non-repudiation and involves the completeness and correctness of data and the correct functioning of the system in which it is processed [20]. 'Availability' covers systems, applications and services as well as the data processed within it means that the systems, applications and services are operational at the defined times and that the data can be accessed as intended [20]. For 'availability', Hoerbst & Ammenwerth [18] indicated four requirements that EHR systems should provide; these are (1) availability of data/information should be ensured, (2) the system should support archiving of data, (3) the readability of archived data should be preserved, (4) deleted data should not be available in the system (e.g. display, export, …). For all attributes together, the adapted list contains 59 qualitative requirements that an EHR system should cover [19] and provides an answer to RQ1.

Supporting structures, we call them 'frameworks' are essential for providing guidelines or assessment tools for a specific use case solution. There are already frameworks that guide the development of EHR systems using Blockchain. A systematic literature

review using keywords such as 'EHR', 'EMR', 'PHR', 'Blockchain', 'Cybersecurity' and 'Framework' or 'Assessment Tool' was conducted. An overview of the found frameworks differentiated according to 'theoretical' and 'operative' solutions is presented in Table 2 and Table 3.

**Table 2.** Theoretical solution proposals for Blockchain used in the EHR field.

| Framework | Reference | Main Feature | Architecture |
|---|---|---|---|
| - | Shahnaz et al. (2019) [28] | Framework focusing on secure storage of EHRs concerning granular access management | Ethereum, three-layer architecture |
| BBDS | Xia et al. (2017) [29] | Data Sharing framework focusing on access control for data in the cloud | Permissioned, three-layer architecture |
| BHEEM | Vora et al. (2019) [30] | Framework focusing on efficient storage and maintenance of EHRs | Ethereum, four components |
| BPDS | Liu et al. (2018) [31] | Preservation of privacy in EMR sharing | Consortium, three-layer architecture |
| DASS-CARE | Al-Karaki et al. (2019) [32] | Framework focusing on healthcare including the management of EMRs | Blockchain in general |
| EACMS | Rajput et al. (2019) [33] | Access control management of PHRs in case of emergencies | Permissioned (Hyperledger Fabric) |
| EMR-Share | Xiao et al. (2019) [34] | Framework focusing on cross-organizational medical data sharing and access management | Permissioned, three-layer architecture + Blockchain network |
| MeDShare | Xia et al. (2017) [35] | Sharing of medical data between cloud service providers | Four-layer architecture |

**Table 3.** Operative solution proposals for Blockchain used in the EHR field.

| Framework | Reference | Main Feature | Architecture |
|---|---|---|---|
| MedBlock | (Medblock, 2017b) [36] | Solution focusing on business-to-business Blockchain protocol implementations, facilitating data analytics | Hyperledger Fabric |
| MedChain | Shen et al. (2019) [37] | User-driven framework for Healthcare data sharing | Dual-network architecture |
| Medicalchain | (Medicalchain, 2019) [38] | Solution focusing on maintaining a single true version of patient data and issuing tokens | Hyperledger Fabric and Ethereum |
| Med-Rec | Azaria et al. (2016) MedRec (n.d.) [39] | System to handle EMRs with mining rewards to medical stakeholders | Ethereum |
| DASS-CARE | Al-Karaki et al. (2019) [32] | Framework focusing on healthcare including the management of EMRs | Blockchain in general |
| EACMS | Rajput et al. (2019) [33] | Access control management of PHRs in case of emergencies | Permissioned (Hyperledger Fabric) |
| EMR-Share | Xiao et al. (2019) [34] | Framework focusing on cross-organizational medical data sharing and access | Permissioned, three-layer architecture + Blockchain |
| MeD-Share | Xia et al. (2017)[35] | Sharing of medical data between cloud service providers | Four-layer architecture |

The findings showed that there is no framework for building Blockchain-based EHR systems in consideration of strong cybersecurity requirements nor specifically for use in Switzerland (regulatory perspective). No found framework did specifically consider (cyber) security. The lack of a means to check whether Blockchain covers the relevant

EHR requirements for cybersecurity constitutes the research gap. Therefore, a cybersecurity requirement assessment tool for its use in the EHR context is sketched, which aims at facilitating the cybersecurity requirements comparison and coverage assessment of Blockchain and other - traditional - (database-based) systems (section 4.2 and resulting artefact in [19]). In the next step, the assessment tool is applied for the use case of EHR in Switzerland. In order to compare and contrast the open-source Blockchain platform 'Hyperledger Sawtooth' as an alternative to the database solution 'Swiss Electronic Patient File' (EPF).

## 4 Use Case: Hyperledger Sawtooth for EHR

Hyperledger Sawtooth, in the following referred to as Sawtooth, is an open-source project under the umbrella of the Hyperledger family hosted by the Linux Foundation [22]. Sawtooth is a modular platform that comes - by default - with robust security functionalities and offers various customizing options, and hence was chosen to represent a relevant Blockchain [23]. Sawtooth is focusing on modularity which allows enterprises so select the suited transaction rules, permissioning and consensus algorithms. While Sawtooth provides its consensus algorithm 'Proof-of-Elapsed-Time' (PoET), it supports the use of other types of consensus algorithms [24]. PoET is based on a random lottery function. A random period is given for each participating node in the network, to which the node must adhere to. The node whose time is the shortest wins the block and can add the block to the Blockchain [25]. Sawtooth differentiates between PoET-'SGX' (Intel® Software Guard Extensions), which requires special hardware to ensure a trusted execution environment, and PoET simulator which can be executed on any type of hardware [24]. Concerning cryptography, Sawtooth uses the secure hash algorithms SHA-256 and SHA-512 as cryptographic safeguards in the transaction process [26]. With the Sawtooth-Ethereum integration project (Seth), it is possible to integrate Ethereum smart contracts to Sawtooth [24].

For our use case, we decided to use EPF - a Swiss, non-blockchain solution for the collection of personal documents with treatment-relevant information from patients. These include, for example, the discharge report of a hospital, the medication list, x-rays or the vaccination card. The EPF does not contain all electronically collected health information, but only those that are relevant for other professionals and further treatment. In addition to the EPF, the health service provider (e.g. the general practitioner) continues to keep a personal medical history, which contains more information than the EPF. The EPF does not contain documents from authorities or health insurance companies. Authorities and health insurers do not have access to the EPF [12]. All persons in Switzerland can request having their data in the EPF. With the EPF, patients can divide their documents into confidentiality levels and can grant and withdraw access to health service providers [12]. The EPF is decentral established; it is an association of regional implementations from various providers. However, the legal requirements and rules are the same throughout Switzerland ('Technical and Organizational Certification Requirements for Communities and Core Communities' [20]). The decentralized approach offers basic security since not all EHR data is stored in a single place. The

Federal Act on EPF stipulates how EPF must be organized and technically secured. Every provider of the EPF is examined, certified, and regularly inspected [12].

### 4.1 Assessment Tool Development

Following the research questions RQ2 and RQ3, the assessment tool is tested by filling in Sawtooth capabilities matching the requirements (resulting artefact in [19]). Subsequently, the results are compared to the Swiss EPF. Categories and unstructured reasonings will be assigned to compare whether Sawtooth or the Swiss EPF cover the EHR system requirements (based on systems documentation). The following listing explains the defined assessment categories:

**Table 4.** Requirements assessment category and their reasoning

| Category | Reasoning |
|---|---|
| Yes | Evidence has been found that the system meets the given requirement. |
| By configuration | The system does not support the requirement by default. However, the requirement can be met with additional tools that enhance the system. For Sawtooth, this means an enhancement of the Blockchain network. |
| By extension | The system does not support the requirement by default. However, the requirement can be met when the system is extended by additional soft- or hardware outside of the system. |
| Organizational | The requirement is unrelated to technology and can be met on an organizational level by following suited frameworks or standards. |
| No | Framework focusing on healthcare including the management of EMRs |
| Unclear | No indication was found that the requirement could be covered by the system, by the configuration of the system, by extension outside of the system or by organizational measurements. |

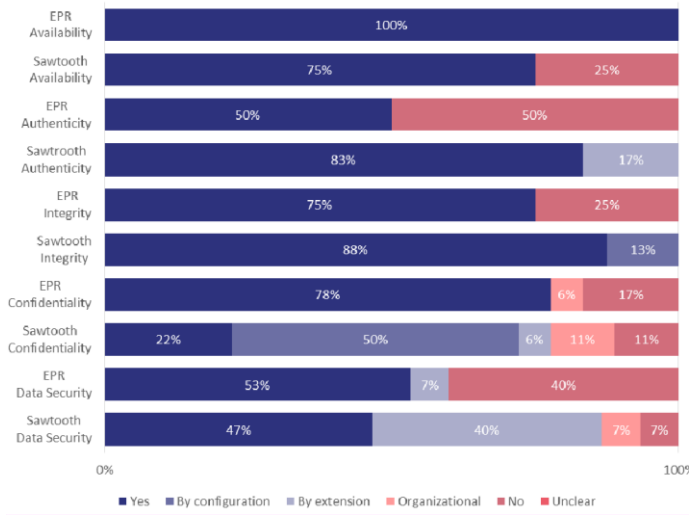
The assignment of the categories in Table 4 to each requirement was carried out in three iterations. For each EHR requirement, a compare and coverage assessment for Sawtooth and EPF was conducted, peer-reviewed and validated by qualitative expert interviews. The experts were selected in the Swiss Blockchain research and the EHR development communities. Unclear requirements were specified by consulting the documentation' Technical and Organizational Certification Requirements for Communities and Core Communities' [21]; this document was used as a basis for assessing the requirements coverage by the Swiss EPF. It is essential to state that, since it is a requirements documentation, a final EPF solution must cover those requirements for certification but can additionally cover more features, e.g., towards cybersecurity. The final and full assessment tool is visible in [19].

### 4.2 Comparison and Coverage

The results of the assessment of the coverage of EHR system requirements by Sawtooth and by the Swiss EPF are visualized in Fig. 1. If only those requirements are

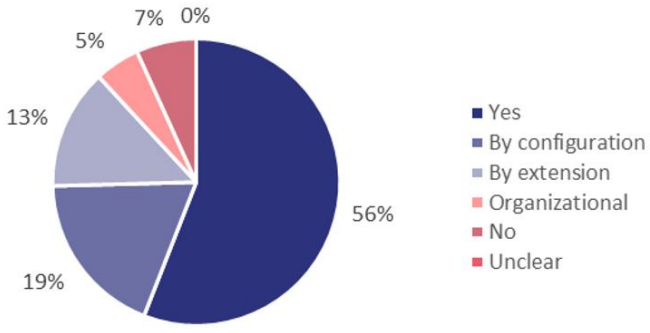
considered that have been categorized as 'Yes', many EHR system requirements that are not covered by default (category 'yes') would be missed.

**Fig. 1.** EHR system requirements coverage by Sawtooth and by the EPF.




Thus, it can be argued that Sawtooth with 55 (93%) covered EHR system requirements more thoroughly than the Swiss EPF with 43 (73%) covered EHR system requirements, when considering the assigned categories 'Yes', 'By Configuration', and 'By Extension'. The individual perspective shows that Sawtooth allows freedom to meet the requirements, either by choosing the right configuration or by relying on an extension (Fig. 2) and only meets a bit more than half of the requirements by default. Although Sawtooth covers the requirements well, it has disadvantages. Sawtooth poorly covers EHR system requirements pointing to the deletion of data. This is also due to the fact of inherent persistency of a Blockchain.

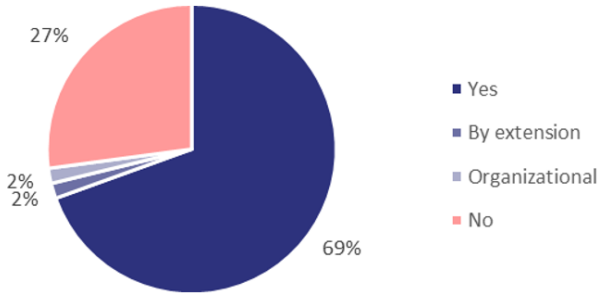
**Fig. 2.** EHR system requirements coverage by Sawtooth.




There are various approaches to handling the issue. One of them is storing data off-chain. It is generally not necessary to store all transaction data on-chain. Data can as

well be stored in another database and be linked by hashes to the Blockchain. Storing data off-chain would enable deletion following the EU GDPR [27]. This would also make sense for big files such as imaging. While Sawtooth covers many EHR system requirements, organizational factors should not be left out. An example is key management, with their critical tasks assigning, storing, and retrieving in case the keys were lost.

**Fig. 3.** EHR system requirements coverage by EPF.




The individual perspective on the EPF shows that the system covers more requirements by default, but has a significantly high number of cybersecurity requirements that are not met at all (Fig. 3). Because it is a system that has to fit into the existing health systems landscape, it allows for less flexibility in its design when comparing to Sawtooth. In conclusion, it can be said that a qualitative and quantitative comparison between the systems is possible. However, the two differ significantly in their architecture primarily since the compare and coverage assessment is based on a document for the Technical and Organizational Certification Requirements for Communities and Core Communities [21] and not on a concrete instance.

## 5 Conclusion and Further Research

The main contribution of this study is the assessment tool proposition as the possibility to assess the coverage of cybersecurity relevant EHR system requirements by Sawtooth and the Swiss EPF both as an exemplary use case. This study first outlined the relevance of EHR in combination cybersecurity requirements and Blockchain as a potential enabling technology. For the foundation, the intersection cybersecurity, Blockchain, and EHR were discussed. Based on that, we developed an assessment tool which considered cybersecurity-related EHR requirements. The assessment tool was subsequently developed and applied to Sawtooth and the Swiss EPF. The comparison showed that Blockchain, and in particular Sawtooth could be used to enable cybersecurity for EHR. However, Sawtooth does not perform well on those requirements where permanent deletion of data is required. Thus, the critical characteristic 'persistency' - a strength of Blockchain in general - is a weakness in the context of EHR or for sensitive data in general. In section 4.2, it was mentioned that there are approaches to solving this problem. Besides, it should be noted that the Swiss EPF also covers many of the

EHR requirements. This means that while Blockchain can be used to enable cybersecurity for EHRs, this can also be achieved with a non-Blockchain based system. In addition to contributing to research, the final assessment tool in [19] could serve EHR custodians for their analysis of system variants.

## 6 References


1. Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System, (2008). Consulted, 1–9. Journal for General Philosophy of Science, (1). https://doi.org/10.1007/s10838-008-9062-0.
2. Zhao, J. L., Fan, S., & Yan, J. (2016). Overview of business innovations and research opportunities in blockchain and introduction to the special issue. Financial Innovation, 2(1), 1–7. https://doi.org/10.1186/s40854-016-0049-2.
3. Gartner. (2018). 5 Trends Emerge in the Gartner Hype Cycle for Emerging Technologies, 2018. Retrieved from https://www.gartner.com/smarterwithgartner/5-trends-emerge-in-gartner-hype-cycle-for-emerging-technologies-2018/.
4. Gartner. (2019). Interpreting technology hype. Retrieved from https://www.gartner.com/en/research/methodologies/gartner- hype-cycle
5. Kshetri, N. (2017). Blockchain's roles in strengthening cybersecurity and protecting privacy. Telecommunications Policy, 41(10), 1027–1038. https://doi.org/10.1016/j.telpol.2017.09.003.
6. Liu, L., & Xu, B. (2018). Research on information security technology based on blockchain. 2018 3rd IEEE International Conference on Cloud Computing and Big Data Analysis, ICCCBDA 2018, 380–384. https://doi.org/10.1109/ICCCBDA.2018.8386546.
7. Taylor, P. J., Dargahi, T., Dehghantanha, A., Parizi, R. M., & Choo, R. (2019). A Systematic Literature Review of Blockchain Cyber Security. Digital Communications and Networks. https://doi.org/10.1016/j.dcan.2019.01.005.
8. Hölbl, M., Kompara, M., Kamišalić, A., & Zlatolas, L. N. (2018). A systematic review of the use of blockchain in healthcare. Symmetry, 10(10). https://doi.org/10.3390/sym10100470.
9. Rabah, K. (2017). Challenges & Opportunities for Blockchain Powered Healthcare Systems: A Review. Mara Research Journal of Medicine & Health Sciences, 1(1), 45–52.
10. IBM Security and Ponemon Institute. (2019). Cost of a Data Breach Report.
11. Ambinder, E. P. (2005). Electronic Health Records. Journal of Oncology Practice, 57–63.
12. ehealthsuisse. (2017). Meine Gesundheitsinfos. Zur richtigen Zeit am richtigen Ort. Meine Gesundheitsinfos. Zur richtigen Zeit am richtigen Ort. Retrieved from https://www.e-health-suisse.ch/fileadmin/user_upload/Dokumente/2017/D/171219_EPD-Broschuere_Bevoelkerung_d.pdf.
13. The Office of the National Coordinator for Health Information Technology. (2019). What are the differences between electronic medical records, electronic health records, and personal health records? Retrieved from https://www.healthit.gov/faq/what-are-differences-between-electronic-medical-records-electronic-health-records-and- personal.
14. Schweizerische Eidgenossenschaft. (2017a). Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz.
15. GDPR.eu. (n.d.). What is GDPR, the EU's new data protection law? Retrieved November 28, 2019, from https://gdpr.eu/what-is- gdpr/.

16. Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter (EDÖB). (n.d.). Schweigepflicht. Retrieved from https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/gesundheit/schweigepflicht.html.
17. Roehrs, A., Da Costa, C. A., Da Rosa Righi, R., & Kleinner, F. (2017). Personal health records: A systematic literature review. Journal of Medical Internet Research, 19(1). https://doi.org/10.2196/jmir.5876.
18. Hoerbst, A., & Ammenwerth, E. (2010). Electronic health records: A systematic review on quality requirements. Methods of Information in Medicine, 49(4), 320–336. https://doi.org/10.3414/ME10-01-0038.
19. Moriggl, P., Asprion, P., Kramer, F. (2020) Appendix. Assessment Tool Application Comparison between a blockchain and a traditional database solution for electronic health records. BES2020. 10.13140/RG.2.2.24736.81924
20. Bedner, M., & Ackermann, T. (2010). Schutzziele der IT-Sicherheit. Datenschutz Und Datensicherheit - DuD, 34(5), 323–328. https://doi.org/10.1007/s11623-010-0096-1.
21. Eidgenössisches Departement des Innern EDI. (2019). Technische und organisatorische Zertifizierungsvoraussetzungen für Gemeinschaften und Stammgemeinschaften. Retrieved from https://www.bag.admin.ch/dam/bag/de/dokumente/nat- gesundheitsstrategien/strategie-ehealth/anhoerung-ausfuehrungsrecht/verordnungen/epdv-edi- anhang2.pdf.download.pdf/08-2_de_epdv-edi_anhang_2.pdf.
22. The Linux Foundation. (2018). Hyperledger Sawtooth. Retrieved from https://www.hyperledger.org/projects/sawtooth.
23. Moriggl P., Asprion P.M., Schneider B. (2021) Blockchain Technologies Towards Data Privacy—Hyperledger Sawtooth as Unit of Analysis. In: Dornberger R. (eds) New Trends in Business Information Systems and Technology. Studies in Systems, Decision and Control, vol 294. Springer, Cham. https://doi.org/10.1007/978-3-030-48332-6_20.
24. Intel Corporation. (n.d.-e). Sawtooth - Introduction. Retrieved from https://sawtooth.hyperledger.org/docs/core/nightly/1- 1/introduction.html?highlight=immutable.
25. Intel Corporation. (n.d.-f). Sawtooth - PoET 1.0 Specification. Retrieved from https://sawtooth.hyperledger.org/docs/core/nightly/1-1/architecture/poet.html?highlight=poet.
26. Intel Corporation. (n.d.-b). Sawtooth - Building and Submitting Transactions. Retrieved from https://sawtooth.hyperledger.org/docs/core/nightly/1-1/_autogen/txn_submit_tutorial.html?highlight=sha.
27. Finck, M. (2019). Blockchain and the General Data Protection Regulation - Can distributed ledgers be squared with European data protection law? Retrieved from https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf.
28. Shahnaz, A., Qamar, U., & Khalid, A. (2019). Using Blockchain for Electronic Health Records. IEEE Access, PP, 1. https://doi.org/10.1109/ACCESS.2019.2946373.
29. Xia, Q., Sifah, E. B., Smahi, A., Amofa, S., & Zhang, X. (2017). BBDS: Blockchain-based data sharing for electronic medical records in cloud environments. Information (Switzerland), 8(2). https://doi.org/10.3390/info8020044.
30. Vora, J., Nayyar, A., Tanwar, S., Tyagi, S., Kumar, N., Obaidat, M. S., & Rodrigues, J. J. P. C. (2019). BHEEM: A Blockchain-Based Framework for Securing Electronic Health Records. 2018 IEEE Globecom Workshops, GC Wkshps 2018 - Proceedings, 1–6. https://doi.org/10.1109/GLOCOMW.2018.8644088.
31. Liu, J., Li, X., Ye, L., Zhang, H., Du, X., & Guizani, M. (2018). BPDS: A Blockchain Based Privacy-Preserving Data Sharing for Electronic Medical Records. 2018 IEEE Global Communications Conference, GLOBECOM 2018 - Proceedings, 1–6. https://doi.org/10.1109/GLOCOM.2018.8647713.

32. Al-Karaki, J. N., Gawanmeh, A., Ayache, M., & Mashaleh, A. (2019). DASS-CARE: A Decentralized, Accessible, Scalable, and Secure Healthcare Framework using Blockchain. 15th International Wireless Communications & Mobile Computing Conference (IWCMC), 330–335. https://doi.org/10.1109/iwcmc.2019.8766714.
33. Rajput, A. R., Li, Q., Ahvanooey, M. T., & Masood, I. (2019). EACMS: Emergency Access Control Management System for Personal Health Record Based on Blockchain. IEEE Access, 7, 84304–84317. https://doi.org/10.1109/ACCESS.2019.2917976.
34. Xiao, Z., Li, Z., Liu, Y., Feng, L., Zhang, W., Lertwuthikarn, T., & Goh, R. S. M. (2019). EMRShare: A Cross-Organizational Medical Data Sharing and Management Framework Using Permissioned Blockchain. Proceedings of the International Conference on Parallel and Distributed Systems - ICPADS, 2018-Decem, 998–1003. https://doi.org/10.1109/PADSW.2018.8645049.
35. Xia, Q., Sifah, E. B., Asamoah, K. O., Gao, J., Du, X., & Guizani, M. (2017). MeDShare: Trust-Less Medical Data Sharing among Cloud Service Providers via Blockchain. IEEE Access, 5, 14757–14767. https://doi.org/10.1109/ACCESS.2017.2730843.
36. Medblock. (2017b). MedBlock. Retrieved from https://www.medblock.co.uk/.
37. Shen, B., Guo, J., & Yang, Y. (2019). MedChain: Efficient healthcare data sharing via blockchain. Applied Sciences (Switzerland), 9(6). https://doi.org/10.3390/app9061207.
38. Medicalchain. (2019). Medicalchain - Blockchain for electronic health records. Retrieved from https://medicalchain.com/en/#mobile-site-navigation.
39. Azaria, A., Ekblaw, A., Vieira, T., & Lippman, A. (2016). MedRec: Using blockchain for medical data access and permission management. Proceedings - 2016 2nd International Conference on Open and Big Data, OBD 2016, 25–30. https://doi.org/10.1109/OBD.2016.1