Federated Electronic Health Records Using a Blockchain

John CHELSOM[a], Luis MARCO-RUIZ [b,1], Øivind SKEIDSVOLL SOLVANG [b,c], Sonja CASSIDY[b,c], Ove LINTVEDT[b], Conceição GRANJA[b,d] and Terje SOLVOLL [b,d]
[a] *Fordham University, New York, USA*
[b] *Norwegian Centre for E-health Research, Tromsø, Norway*
[c] *Helse Vest IKT, Department of Strategic ICT, Bergen, Norway*
[d] *Faculty of Nursing and Health Sciences, Nord University, Bodø, Norway*

Abstract. The Valkyrie project aims to develop a demonstration Federated Electronic Health Record for the use of mental health practitioners in Norway. Information for the record is drawn from existing records in Source Systems operating across primary and secondary care. Recording of information in any such system, in response to a healthcare event, triggers the generation of an Encrypted Token, containing summary metadata about the event, clinical coding indicating its clinical context and a locator that can be used to retrieve the full record of the event from the original Source System. The Valkyrie architecture consists of a number of interlinked Security Domains, each with its own private and public keys, through which the Encrypted Tokens are passed. Each Security Domain performs a specific function on a set of Tokens and only has access to the information within each Token that is necessary to perform that function. This paper describes the structure of the Encrypted Token, the function of each Security Domain and the orchestration of the flow of Tokens through the Domains. Together this allows a user to run a Valkyrie Session, in which they can view the content of a patient record, where all content has been drawn in real-time from heterogenous Source Systems (ISO13606- and openEHR-based) and is destroyed when the session terminates.

Keywords. Federated Electronic Health Record, Blockchain, PKI, ISO 13606, openEHR, Care Pathway.

1. Introduction

Fragmentation of current health information systems jeopardizes the continuity of care for patients who undergo complex paths involving several health organizations. This is particularly evident in mental healthcare, where patients need specialized services (i.e., psychologists and psychiatrists) and primary healthcare. This context exacerbates the existing challenges in making different healthcare organizations interoperate as a digital ecosystem to ensure continuity of care [1,2]. The health information systems (HIS) used to support these patients are often behind organizational firewalls and, in countries like Norway, protected by enhanced privacy access rules that restrict access to patient's Electronic Health Records (EHRs) to those directly involved in the patient's treatment. These challenges translate into the main actors involved in mental healthcare not being

[1] Corresponding Author: Luis Marco-Ruiz; E-mail: luis.marco.ruiz@ehealthresearch.no.

able to access each other's patient information. Furthermore, this hampers the design of the optimal care plans requiring coordination between somatic and mental healthcare. In Norway, most hospitals are transitioning to an openEHR-based EHR [1,3], while primary care offices rely on EHRs from several providers. This diversity of HIS poses significant barriers to continuity of care. To tackle this challenge, the Valkyrie project aims to design a Virtual Federated Health Record (VFHR) summary where patient information from several organizations can be tracked and eventually accessed if the appropriate permissions and legitimacy are in place [4]. The Valkyrie concept aims to maintain a trustworthy tracking system of metadata about the information contained in each data source available. The challenge of managing all this information from heterogeneous sources arises at different points in time without a centralized authority keeping track of them. Hence, the Valkyrie infrastructure has to be technology-agnostic and non-invasive so the health organizations continue operating their EHRs normally. This leads to the need for a distributed electronic ledger that reliably stores the timestamp determining when a specific clinical document was created and the organization where it is located. The overall objective of Valkyrie is to make a VFHR summary available to Mental Health practitioners during their encounters with patients. This VFHR summary may be tailored to the clinical context of the patient-practitioner encounter so that only relevant and necessary information is accessible. The high-level architecture of Valkyrie is shown in Figure 1. The VFHR summary represents the full patient record distributed across all the source EHRs. The source EHRs already exist in both primary and secondary care providers across Norway, and have each created fragment (electronic document) of the patient's information stored. Through the VFHR summary, the practitioner can gain access to view any healthcare Event in the federated record; the view of each event is pulled from the source EHR and exists in Valkyrie only for the duration of each session between patient and practitioner.

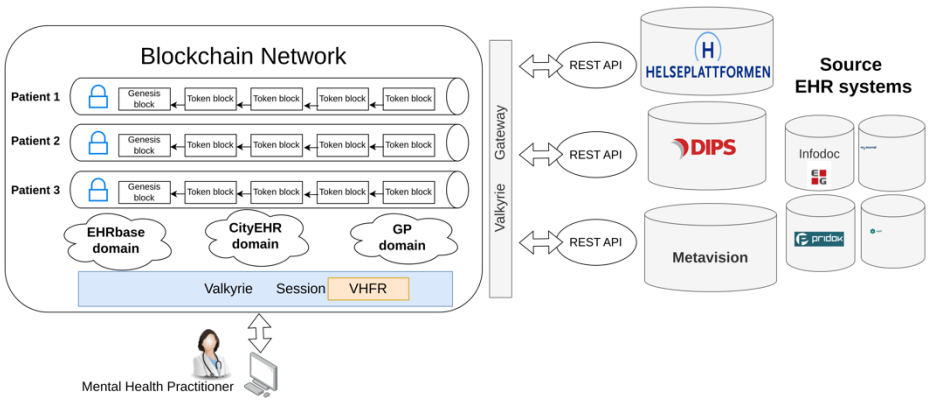

Figure 1. High Level Architecture of Valkyrie.

2. Methods

2.1. Encrypted Tokens and Blockchain

Each Source EHR, whether in primary, secondary or tertiary care, operates within its own Security Domain, with its own private and public key. Encrypted Tokens, contain the summary of the clinical information relevant to one healthcare Event. Whenever a healthcare Event is recorded, the Encrypted Tokens are generated within these domains and then passed out through an Integration Engine to the Token gateway. Encrypted Tokens are generated by the Source EHR systems whenever information is recorded for an Event in the patient's healthcare. The Event will have been recorded as a Composition in ISO-13606-based systems, as a ClinicalDocument in HL7 CDA, as an openEHR Composition in openEHR systems, or as a view formed as the result of a database query in other types of EHR. The Token contains: 1) The Patient Identifier which uniquely identifies each patient across all clinical settings; 2) The Session Parameters instantiated by the Context Manager; 3) The Event description summarizing clinical data. The Encrypted Tokens are stored in a private, centralized blockchain. There is one blockchain for each patient, with the genesis block representing the registration event for the patient in the Valkyrie EHR and the following blocks representing health events. The Patient Ledger contains a registry of each patient known to Valkyrie, with a link to the current block in the patient's blockchain. Thus, the Patient Ledger is the key to the full Tokens blockchain stores for any patient. The blocks added to the Patient Blockchain are encrypted using the public key of the Patient Domain, since this is the domain in which they will be processed.

2.2. Flow control

When a patient is registered with Valkyrie, a new record is created for that patient in the Valkyrie virtual EHR by recording the registration event. Whenever a new event is recorded, an Encrypted Token is generated and passed out through an integration engine running. The tokens are sent by the integration engine to the Valkyrie Gateway, which holds the public keys for each EHR Source. The Valkyrie Gateway is responsible for storing tokens in the patient blockchain. On receipt in the Valkyrie Gateway, the token is decrypted, and the patient identifier is checked in the Patient Ledger. Mental health practitioners log on through the Valkyrie client user interface and are authenticated to start a session with the Valkyrie Server, which is hosted in the Valkyrie Session Domain. During a session a practitioner may: register a new patient in Valkyrie; remove a patient from Valkyrie; view the VFHR for the patient; interact with the patient record held in the VFHR. Within the Token Gateway Domain, the elements inside the Token are encrypted using the public keys of the security domains nominated to process that element. Once a token is received and has been associated with a patient, it is sent from the Token Gateway, where it is added to the end of the blockchain for that patient and the Patient Ledger is updated to reference the newly added block. Each Valkyrie session run by a Mental Health Practitioner is for a designated patient. This means that a session is exclusive to a single encounter between a patient and a practitioner, for example a clinic consultation. For each session, Valkyrie constructs a virtual record for the patient by accessing the Tokens in the Patient Blockchain. This virtual record is viewed within the

Valkyrie Client, using information on Events in the patient's federated record that spans all Source EHR systems where information is stored for the patient. The virtual record is held for the session within the VFHR, using an outline created from the Patient Blockchain.

3. Results

Currently, Valkyrie is in development, having completed a Minimal Viable Product implementation, whose architecture is shown in Figure 1. From the bottom-up, the image shows the EHRs involved. EHRbase[5] is used as the openEHR repository. Due to its compliance with openEHR, it is fully interoperable with the hospital EHR DIPS Arena. The second EHR used is CityEHR[6], which supports storing compositions that are compliant with ISO13606 or HL7 CDA documents. A Mirth Connect instance connects EHRs to the Valkyrie Gateway. It allows the tokens from the different EHRs to be routed to the token gateway and the blockchain network. When a new composition is stored in any EHR, the token is produced and sent to the integration bus, which delivers it to the Valkyrie gateway and a Hyperledger Fabric network. The Hyperledger Fabric network contains one channel for each patient registered in Valkyrie. These are different from communication channels. Instead, they are private subnetworks for communicating blockchain contracts between organizations, (i.e., security domains). Each organization must be authenticated by a membership access provider (e.g., Certificate Authority) to access the channel and execute the transactions that persisted in a ledger only available to channel-authenticated members. No information from the ledger containing patient tokens is shared outside its channel. This guarantees that only doctors treating the patient have access to the patient tokens in the ledger.

4. Discussion and Conclusions

After significant investments in interoperability and data integration [7], the healthcare domain has shown that disparities among HIS will always be present due to the different needs of healthcare levels and professionals. New architectures that allow dealing with this diversity are needed to guarantee continuity of care beyond patient summaries [2]. Valkyrie leverages the latest developments in blockchain to enable a VFHR. Blockchain allows privacy and access control to healthcare even without a central authority. This is particularly convenient when several health levels and organizations must participate in patient healthcare. Haddad et al. [8] proposed a blockchain architecture based on Ethereum to store health data in the Interplanetary File System. Valkyrie architecture shares commonalities with the one proposed by Haddad et al. such as the tokens summarizing the content in the EHR. However, Valkyrie adopts a different approach by advancing the integration of information from heterogeneous EHRs, which use different standards (such as ISO, HL7, and openEHR) that belong to different healthcare levels and organizations, while Haddad's work focuses on algorithmic efficiency.

References

[1] Pedersen R. Establishing ICT Governance for Regional Information Infrastructures in Healthcare | Request PDF [Internet]. ResearchGate. [cited 2019 Jan 7]. Available from: https://www.researchgate.net/publication/301281301_Establishing_ICT_Governance_for_Regional_Information_Infrastructures_in_Healthcare

[2] Raab R, Küderle A, Zakreuskaya A, Stern AD, Klucken J, Kaissis G, et al. Federated electronic health records for the European Health Data Space. Lancet Digit Health. 2023 Nov;5(11):e840–7.

[3] Pedersen R, Marco-Ruiz L. Chapter 19 - Evidence-based biomedical information systems: The road ahead. In: Hovenga E, Grain H, editors. Roadmap to Successful Digital Health Ecosystems [Internet]. Academic Press; 2022 [cited 2022 Apr 7]. p. 437–55. Available from: https://www.sciencedirect.com/science/article/pii/B9780128234136000100

[4] Solvoll T, Granja C, Cassidy S, Solvang O, Lintvedt O. Valkyrie: A Distributed Service-Oriented Architecture for Coordinated Healthcare Services. 2023.

[5] EHRbase – Ready for Action [Internet]. [cited 2020 May 22]. Available from: https://ehrbase.org/

[6] cityEHR | Seven Informatics [Internet]. [cited 2024 Mar 7]. Available from: https://seveninformatics.com/cityehr/

[7] Sheikh A, Anderson M, Albala S, Casadei B, Franklin BD, Richards M, et al. Health information technology and digital innovation for national learning health and care systems. Lancet Digit Health. 2021 Jun;3(6):e383–96.

[8] Haddad A, Habaebi MH, Elsheikh EAA, Islam MR, Zabidi SA, Suliman FEM. E2EE enhanced patient-centric blockchain-based system for EHR management. PloS One. 2024;19(4):e0301371.