Summer 2021

Temporary Access to Medical Records in Emergency Situations

Zhi Chen

Samaneh Madanian

Farhaan Mirza

Temporary Access to Medical Records in Emergency Situations

Zhi Chen
Auckland University of Technology (AUT)
rgk3484@autuni.ac.nz

Samaneh Madanian
Auckland University of Technology (AUT)
Sam.madanian@aut.ac.nz

Farhaan Mirza
Auckland University of Technology (AUT)
Farhaan.mirza@aut.ac.nz

Abstract
Access to patients Electronic Health Records (EHR) is a daily operation in mainstream healthcare. However, having access to EHR in emergencies while is vitally important to save patients' life, it could potentially lead to security breaches and violating patients' privacy. In this regards, getting access to patients' medical records in emergency situations is one of the issues that emergency responder teams are facing. This access can be temporary until patients reach hospitals or healthcare centers. In this paper, we aim to explore different technology-based solutions to give responders temporary access to patients' medical records in emergency situations. The core of this study is patients and responders authentication methods that can save precious emergency time and protect the privacy and confidentiality of patients data to the utmost. We also have explored control access mechanism and security audits to increase the security of the procedure and patient privacy.

Keywords: Emergency, Temporary Access, Authentication, Access Control.

1. Introduction
Electronic health record (EHR) and Electronic medical records (EMR) are important to resource in delivering healthcare. EHR is a digital version of the patient's standard clinical data. EHR is a patient-centric real-time record that allows authorized users to obtain information immediately and safely (Tavares & Oliveira, 2016). On the other hand, EMR constitutes data from electronic medical applications and is the data source of patients' EHR (Enaizan et al., 2020). It consists of the medical and treatment history of a patient for episodic healthcare or clinical events. As these systems contain all longitudinal information of patients' health background and history, they that can be a valuable source of information for clinical decisions and play a vital role in providing effective healthcare, especially in emergency situations.

In emergencies, a responsive emergency system plays a vital role in saving patients' lives in time. For decision support in emergencies, emergency responders and other involved parties should have timely and accurate medical information to provide swift rescue and appropriate medical interventions. At the same time, patients health and medical information should be protected against any potential privacy breaches. Therefore, based on patients' health circumstances and involved medical teams, different role levels authority, system privileges, and data access levels should be defined to provide clear, readable and practical information while protecting patients' privacy.
Although different countries have different legislations to regulate and manage EHR and EMR, there are different arrangements when it comes to emergencies. The main reason is to avoid personal injury or death due to the inability to obtain the patient's medical information in time,

an action that violates the normal work process taken (Wickramage, Fidge, Sahama, & Wong, 2017). Similarly, based on the Health Insurance Portability and Accountability Act (HIPAA), in emergency situations, even if there is no relevant data usage authority, the government has authorized medical workers to decrypt any patient-related data (T. Chen & Zhong, 2012).

In this regard, the concept of *Temporary Access to Medical Record* (TAMR) in emergency situations has emerged. In these situations, data availability is more important than security and confidentiality, and EHRs are also obliged to provide critical data for medical providers involved in emergency care (Wickramage et al., 2017). However, effective authentication methods to quickly obtain relevant patients' information within their respective authorized scope can reduce and even prevent cybersecurity incidents.

The fundamental motivation of this paper is to explore authentication and access control mechanisms available for temporary access to EHR, to conduct this exploratory work we conducted a literature review looking into security in medical information systems, access control, and auditing. On the basis of our literature search we postulate a feasible mechanism to find patient information in emergencies without compromising patients' privacy.

2. Research Background

There is an exponential interest in EHR security and privacy. However, not many research studies have been done on TAMR in emergencies and the security and privacy of patients' medical records. This makes EHR utilization uncertain in emergencies, as it is not clear how emergency responders should get patients' consent and access to medical records.

Therefore, TAMR has attracted research interests, recently. TAMR focuses on three aspects: (i) EHR system with a uniform format, clear structure and standardized definition. (ii) security and confidentiality of patient medical records; (iii) comprehensive, flexible and secure access control system. Our *research problem* deals with having patients' medical background and timely access to the information is vital in emergency situations and help the responders' team to save precious time and get more accurate medical decisions (Ben-Assuli, Sagi, Leshno, Ironi, & Ziv, 2015). Our *research question* therefore is: Can we can propose a solution to deal security and access control in parallel manage patient privacy while accessing their EHR in emergencies. Our research solution (presented in section 3) is a proposed system design catering for three scenarios: conscious patients, unconscious patients, and disaster scene. The implications of security, access, and privacy vary for these three scenarios, therefore an effective solution should manage TAMR accordingly. The following sections introduce some background literature.

2.1 Security in Medical Information Systems

Different security mechanisms have been proposed for EHR systems. To cope with the conflict of requirements for balancing speed and safety in emergency medical situations, separating emergency data from the EHR system is proposed (Darnasser, 2013). This approach could be useful to minimize the amount of leaked data in the event of emergency access violations. Cloud services that provide reliable distributed storage approach can improve the EHR system's security and reduce information exchange time (Alamir, Raman, Alhashimi, Almoaber, & Alremeithi, 2019). However, to enhance security, ubiquitous security access through a palm vein pattern authentication system is suggested (Alamir et al., 2019). In another study, Digital Rights Management (DRM) and digital certificate technologies were proposed for EHR sharing and clinical integration system in the cloud (Y. Y. Chen, Lu, & Jan, 2012). These systems could

use non-repudiation digital signatures, to enhance confidentiality and discover problems through audits.

More recently, a biometric-based Blockchain is proposed to improve EHR access while maintaining patient privacy and identity security (Baqari & Barka, 2020). The natural decentralization of the Blockchain and its cryptographic services makes it a potential medium for communication between the cloud EHR systems and users. The patient's identity cannot be traced back to a specific EHR record.

2.2 Access Control in Medical Information System

Privacy is an important challenge in the medical systems and access control can be the main mechanism for protecting patients' privacy (Eikey, Murphy, Reddy, & Xu, 2015). In emergencies, the goal is satisfying the need to maintain the privacy of EHR and the need to access these records (Gardner, Garera, Pagano, Green, & Rubin, 2009). Therefore, an *access control system* would be an effective and realistic approach to protect patient privacy and confidentiality and obtain patient data in an emergency. This access can be controlled in the following three layers:

2.2.1 Identity Authentication

Identity authentication is to confirm medical team identity and patients, and their legitimacy through the identification service. The purpose is to establish an end-to-end secure link between both parties through authentication. In this regard, Khan and Sakamura (2016) proposed eTRON tamper-resistant cards to authenticate users. The system uses public-key encryption technology to achieve identity verification and tamper resistance. The public key certificate is provided by the eTRON certification authority. Compared with smart cards that use a shared key, this system is more secure as the tamper-resistant function can resist physical and man-in-the-middle (MITM) attacks and prevent copying and modification.

A finger-based system to identify patients in emergency situations and obtain EHR access is proposed by Choosang and Vasupongayya (2015). Palmprints is suggested in Karthikeyan and Sukanesh (2012) due to their higher recognition accuracy in comparison with fingerprints and more secure than smart cards. The combination of facial and fingerprint recognition and password for Emergency Medical Technicians (EMT) is proposed in (Gardner et al., 2009) for authorization of EHR access in general and emergencies. In the proposed system, patients' data are securely stored on a smartphone and available for emergency responders even if the patient is unconscious.

Recently, Jayanthy, Anishkka, Deepthi, and Janani (2019) designed a system for facial recognition for confirming patients' identity. This system performs accurate facial recognition and replaces the unified health code with facial recognition technology. In another study, face and eye recognition, QR Code and fingerprint are suggested for user authentication (Sandamal et al., 2019). This comprehensive method is based on biometric access control and could be promising in identifying patients and balancing the system's flexibility and security by restricting the contents of the medical records that can be viewed in an emergency.

Some other technologies are also proposed for authentication purposes. NFC is proposed for identity authentication and EHR storage system access (Sethia, Gupta, Mittal, Arora, & Saran, 2014). An Android application is developed to access NFC tags and to perform close-range data reading and identity authentication. In another study, an augmented card system based on

augmented reality technology (RA) is proposed to recognize RA markers and confirm the identity (Ierache et al., 2016).

2.2.2 Access Control Strategies

Access control is used to restrict access capabilities and scope, limit access to key resources and prevent illegal users from intruding, or damage caused by legitimate users' improper operations. This enhances the safety and legal use of medical information. To ensure the medical data access, a red-alert protocol is proposed by (Oliveira, Michalas, Groot, Marquering, & Olabarriaga, 2019). In this approach, medical providers can only visit patients' data within the time required to complete specific procedures related to the patient's condition (e.g., transfer of patients to the hospital). Although this approach provides high security in access data, it has low availability in difficult situations.

Sicuranza and Esposito (2013) summarized access control models based on Mandatory Access Control (MAC), Discretionary Access Control (DAC) and Role-Based Access Control (RBAC). RBAC has greater flexibility than MAC and easier to handle than DAC. In their research, based on RBAC, a multi-level patient privacy attribute model was designed which is a fine-grained access model in line with the main security requirements of the EHR system. By defining purpose, checklist, time and restriction components the system administrator can dynamically manage document access that puts patients' privacy in the centre.

RBAC was combined with the contextual-attribute-based access control (ABAC) model to design a more flexible and dynamic RBAC model (Khan & Sakamura, 2016). This model also embodies the design ideas of dynamic, temporary and patient privacy and safety in the centre. However, the best privacy protection strategies in EHRs are segmentation, isolation, separate management, and e-consent, aiming to fine-tune sensitive medical records according to predefined standards (Rothstein, 2012). By improving the RBAC model, the goal of EHRs access control, the balance of security and ease of access, can be achieved.

2.2.3 Security Audit

The widespread application of EHRs has increased the need for a health information log audit mechanism to prevent deliberate or unconscious destruction and abuse of health information (Wickramage et al., 2017). Such audit requirements are more needed in emergency situations. Wickramage et al. (2017) in their research defined log files with additional information and applies them to the audit process to monitor deviations in the expected sequence of events during health care emergencies.

King, Smith, and Williams (2012) proposed a user-based non-repudiation audit mechanism. By studying the impact of 16 types of conventional auditable events on non-repudiation, focusing on the specific auditable events of protected health information, the non-repudiation of audit logs was improved. Khan and Sakamura (2016) believe that because the delegation token contains the subject's eTRON ID in its file access control block, the access control delegation log can be audited so that the system has stronger medical privacy protection.

3. Proposed System Design for Medical Emergency System

Having patients' medical background and timely access to the information is vital in emergency situations and help the responders' team to save precious time and get more accurate medical decisions (Ben-Assuli, Sagi, Leshno, Ironi, & Ziv, 2015). In this regards, a responsive emergency system can play a vital role in saving patients' lives by allowing emergency participants to obtain the patient's medical records in a timely manner. This emergency system

grants patients' medical record access to emergency responders. Therefore, it can be assured that medical responders have access to the vital health records in emergencies that save time and support appropriate medical interventions.

On the other hand, the research and realization of the task of temporarily obtaining medical records in emergencies mainly need to focus on three aspects. The first is the participants in the whole process; the second is the definition of the information of medical records in different contexts and how to obtain it; the third is the authority and security of data. Clear definition and thoughtful planning of the above issues are the fundamental way to complete this task effectively. These areas are discussed and covered in this section.

In an emergency, different stakeholders or participants need temporary access to patient medical information in addition to the hospital's emergency system. This includes: (i) Ambulance service; (ii) Rapid Response Team (RRT); (iii) Medical Assistance Team (MAT); and (iv) Trained first aid. In different countries, we may have different involved parties might be different based on the healthcare structure and hierarchies. However, RRT is now a standard configuration in many modern hospitals. RRT in hospital wards is to examine patients with clinical deterioration in emergency situations to reduce morbidity and mortality in the hospital (Orosz et al., 2020). MAT is a disaster medical assistance team comprises doctors and nurses from different clinical sub-specialities, but mainly from emergency and rural medicine or general departments. Trained first aids are the first-aid measures that bystanders can use, do not need or rarely need medical equipment, and take emergency and critically ill patients.

Based on the introduction to existing EHR systems and emergency requirements, it is clear that the proposed system should be based on the current EHR system to authorize and provide corresponding medical information for different participants by effective verification method. Therefore, the focus of our proposed system is the timely authorization of medical providers for temporary access to medical records in an emergency situation, under the premise of ensuring the safety of patient health information as much as possible.

3.1 Identity authentication

The first step in emergency response and accessing patients medical record would patients identification. In this regard, according to different situations and patients' identity, it is necessary to provide a suitable mechanism and method to identify and authorize different participants and groups involved in emergencies, including patients. In the following sub-sections, an introduction to the procedure and the possible technologies utilization for the authentication system is provided. The overall steps and their sequence of identity authentication are presented in Figure 1.

3.1.1 Conscious Patients

If patients are conscious, they can confirm their identity and authorize emergency responders to have access to their medical records. However, some security mechanisms can be used to provide further privacy protection. For example, to support the authorization process and manage the security and privacy of patients' records, a variety of technologies can be leveraged for EHR access including fingerprint, passwords or faceID. As the system response time is important in emergencies, based on the research results none of these technologies significantly increase the response time of the system (Sun, Zhu, Zhang, & Fang, 2011; Zhang, Zang, & Tian, 2015). Encryption technology can be also useful to prevent any data security hacks and replay attacks.

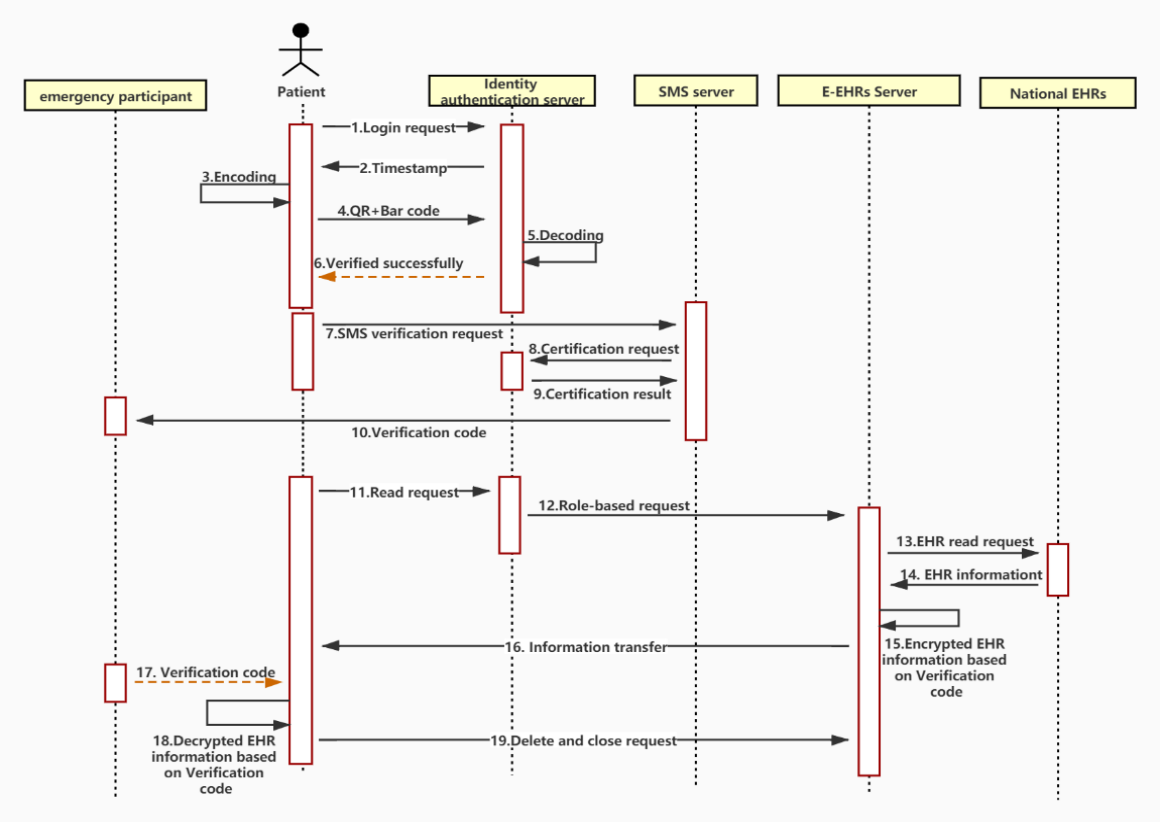

Figure 1: Sequence Diagram of Patient Identity Authentication in Emergencies

3.1.2 Unconscious Patients

The most challenging situation in emergency response is when the responders are dealing with unconscious patients. In these situations, knowing patients' health background and having access to medical records could be a matter of life and death. However, these patients cannot communicate their medical conditions and they are also physically incompetent to retrieve their health records or authorize the emergency responder teams (Sun et al., 2011).

Different approaches have been introduced for these situations such as emergency contact group or trusted users by (T. Chen & Zhong, 2012) and (Thummavet & Vasupongayya, 2013) to authorize emergency responders. However, these approaches take precious time and might be not effective. Therefore, proper technology-based security and privacy mechanisms are required to prevent any misuse of medical data and protect patients' privacy while enabling the responder to have access to patients' medical records.

For this purpose, temporary access to patients' medical background can be provided by using different technologies in parallel with proper patients and response team identity authentication. As patients are unconscious two separate procedures for identity authentication and verification are required, one for the patient and one for the emergency responder. Patient's identity verification in parallel with the responders' identify authentication helps to determine whether the patient's encrypted medical records can be viewed by the responder or not. This double parties identity identification and authentication can prevent any unauthorized access to patients' medical records while supporting emergency responders to have the access to patients' medical history to save a life.

To have such a system in emergencies, EHR systems should capture patients' fingerprints or other biometric identifiers when they set up for a patient. At the same time, there should be a

database system for emergency responders with their staff ID, biometric identifiers and mobile phone numbers. These elements can be used in emergencies for patients and responders identity authentication. This set of mechanisms is believed to improve the access performance of EHR without sacrificing patient privacy and identity security.

Based on these elements we can use either text messaging approach or biometric capturing technologies in emergencies. For example, staff ID and mobile phone number of the responder can be sent to the central server to authenticate the responder and getting a verification code via text messages to grant the temporary access to the patients EHR. This approach maximizes controlling information access in the shortest time while preventing MITM attacks. In more advance systems, biometric (e.g. fingerprint) authentication could be used to authenticate the responders and granting access to patients medical records. As such authentication process includes a timestamp, it can prevent replay attacks and match the patient's identity more accurately. A proposed system workflow is demonstrated in Figure 2.

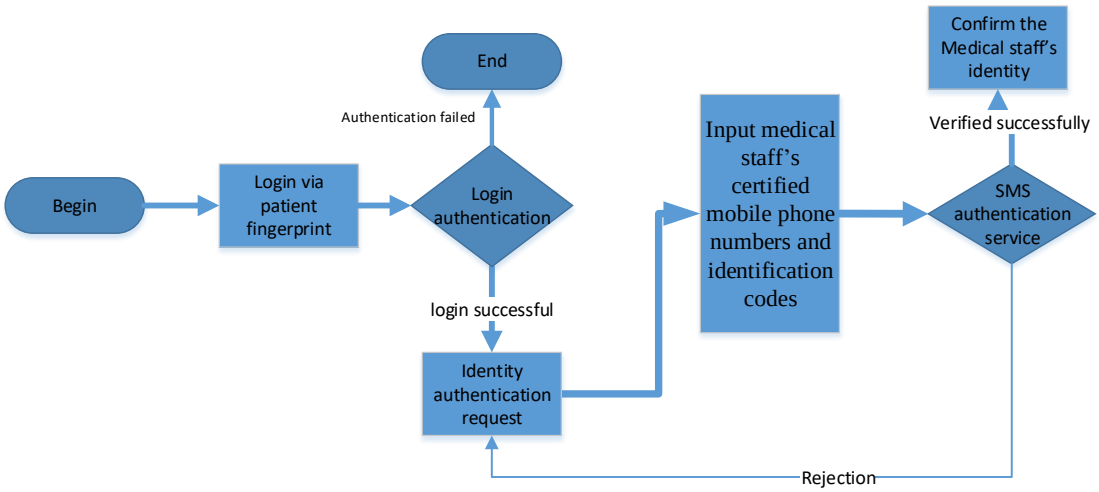

Figure 2: Proposed System Flow for Responders and Patients Authentication

On top of this system, there can be lightweight cryptography models to provide an extra secure system against data breaches.

Other technologies such as physical cards empowered with QR Codes or barcode can be also used in this scenario. Nevertheless, their effectiveness can be less than biometric identification, as they are easy to lose or forget to carry.

3.1.3 Disaster scene

In disaster situations, the number of patients in need of emergency treatment normally surpasses the available disaster responders and other healthcare resources. As saving emergency time and patients' lives should be the most important principles, the system should be designed to accommodate the situation requirements.

In disaster situations, biometric identifications both for disaster casualties and responders is more appropriate due to quick system run up and verification time. The system can be designed with time-limited temporary authorization access.

3.2 Access control

Access control is a necessary and important mechanism to keep patients' health record secure and confidential. At the same time, access control systems must be robust and flexible (Khan

& Sakamura, 2016). To protect the privacy and confidentiality of patients, it is necessary to adopt RBAC and DRM-based information encryption technology. Defining the role, time, and corresponding authority of each person who accesses the patient's medical records can prevent patient information from being leaked or abused by authorized personnel. Moreover, in the process of information acquisition, the information encryption of the patient's medical records based on the license system can prevent information from being stolen or MITM attacks.

As suggested by Darnasser (2013), the idea of separating emergency data from EHR can further improve the privacy of data in this stage. Moreover, restricting the contents of the medical records that can be viewed in an emergency can enhance security (Sandamal et al., 2019).

For effective access control, it is recommended that the EHR system should be based on the HL7 and FHIR information model for the data exchange standard. In the discussed cases, and based on the involved medical teams, the semantic and structural composition of the patient's medical record is expressed in the form of HL7 FHIR standard, and the patient's medical record is called according to the role attributes based on the XML format. Moreover, each request only retrieves medical information related to the role's requirements. The information can be based on default classification or customized by patients.

In the default classification, the calling system classifies EHR information according to categories such as demographics, medical, surgery and lab test backgrounds. The main purpose is to separate the vital information required for rescuers' medical decisions from other information through classification. This information can help rescuers have the most understanding of the patient's situation in the shortest time and take effective rescue measures based on this information.

In contrast, the customized classification by patients is a patient-centred design, as one of the core ideas of today's EHRs. Patients can share the medical information they want to share according to their actual situation and hide some basic information according to their own wishes. For example, patients can choose whether to display the patient's name and address when sharing personal medical information. They can also share their own operation records and X-rays taken due to fractures to emergency personnel through a customized function. It can more effectively help emergency personnel to decide on rescue measures while protecting personal privacy to the greatest extent. To prevent some key emergency information from being hidden due to the limited medical knowledge of the patient, the customized function is only effective for the limited information classification.

3.3 Log Audit and Information Access Sequence

Since in emergencies, time is precious and saving the lives of patients is the first priority, so sometimes it is necessary to compromise between protecting the privacy and saving time. Therefore, the after-the-fact audit system is particularly important in emergency access to the patient's medical record system. A reasonable audit system can effectively prevent the patient's EHR from being misused accidentally or deliberately.

Under normal circumstances, the role of the after-the-fact audit is to find abnormal log records in normal operations and make corresponding identifications or prompts. However, in emergencies, the audit log becomes more complex, and the incompleteness and inconsistency of the log record increase the difficulty of log auditing. Therefore, there is a need to conduct an effective log audit of privacy violations and improve the log recording and presentation

mechanism. Need to add information items for the audit log to help improve the audit log and help the system make correct analysis and inference. This also matches the idea of RBAC.

The enhanced audit log mainly needs to answer several questions: who, when, what, and how. Based on these four log entries, privacy violations can be identified and inferred. Besides, the patient can add three emergency contacts in the application as additional monitors for the log information. To save emergency time, it is unwise to add emergency contacts as authorized persons for access control in some studies. Doing so will invisibly increase the waiting time and waste precious treatment time. But using emergency contacts as log reviewers is a good choice. When the system sends patient medical data to emergency personnel with access rights, it will send the access behaviour to the emergency contact person designated in advance by the patient in the form of a short message, which can help the system better detect unauthorized access to medical records.

4. Discussion and Conclusion

The focus of this paper is how technology can facilitate to authenticate patients identification and emergency responders to grant patient medical information access for emergency purposes. This access is temporary until patients transfer to medical facilities. In this research, besides authentication, we have explored role-based access control and log audits to enhance the security and privacy for patients in providing the emergency responders with medical information for. These tasks are based on the premise that standard medical information can be obtained from EHR systems.

In this article, we have explored some potential technological solution to access patients' data in emergencies in three scenarios: conscious patients, unconscious patients and disaster situation. Among the explored solutions, TAMR based on biometrics identifiers, such as fingerprints, is more promising due to short time for system runup and higher accuracy in identity identifications. However, it is necessary to verify the identity of participants through multiple authentication methods. Therefore, besides biometric identifications for patients, other approaches such as SMS verification was also explored and suggested that can enhance the reliability of identity authentication. The combination of biometric and SMS for patients and responders authentication in an emergency would be an effective, convenient, and easy-to-implement verification method that can enhance system security. This technology integration for verification strengthens the recognition accuracy and security of the system without significantly extending the system login time. Furthermore, SMS verification codes, while enhancing the reliability of identity authentication, try to solve the emergency time as much as possible.

To control access to patients' records, RDAC is proposed. Through the RDAC mechanism, different emergency personnel, regardless of their role, will have enough information required emergency diagnostics and treatment. With RDAC the function of patient customized information is increased, which increases the system flexibility. Adding additional information (who, when, what, how) to the audit log logically helps the log audit system determine privacy violations. Add an additional emergency contact system to help the system find abnormal behaviours through emergency contacts set by patients in advance.

Based on the identity verification method and role-based EHR information acquisition method mentioned above, the identity authentication of emergency participants can be strengthened through the SMS verification system and fingerprint verification system; the security protection during the information transmission process can be strengthened through the fingerprint and different encryption techniques. In this case, the patient's privacy is protected

to the utmost extent through role-based access control. By adding emergency contacts and standardizing audit logs, the audit mechanism is improved, and measures to protect patients' EHR are strengthened. The future development direction of this field should focus on establishing a unified nationwide EHR access system in emergency situations.

References

Alamir, O., Raman, R., Alhashimi, A. F., Almoaber, F. A., & Alremeithi, A. H. (2019, 20-21 Nov. 2019). *M-Blocks (Medical Blocks): A blockchain based approach for patient record management using IBM Hyperledger.* Paper presented at the 2019 Sixth HCT Information Technology Trends (ITT).

Baqari, M. A., & Barka, E. (2020, 15-19 June 2020). *Biometric-Based Blockchain EHR System (BBEHR).* Paper presented at the 2020 International Wireless Communications and Mobile Computing (IWCMC).

Ben-Assuli, O., Sagi, D., Leshno, M., Ironi, A., & Ziv, A. (2015). Improving diagnostic accuracy using EHR in emergency departments: A simulation-based study. *Journal of Biomedical Informatics, 55*, 31-40. doi:https://doi.org/10.1016/j.jbi.2015.03.004

Chen, T., & Zhong, S. (2012). Emergency access authorization for personally controlled online health care data. *J Med Syst, 36*(1), 291-300. doi:10.1007/s10916-010-9475-2

Chen, Y. Y., Lu, J. C., & Jan, J. K. (2012). A secure EHR system based on hybrid clouds. *J Med Syst, 36*(5), 3375-3384. doi:10.1007/s10916-012-9830-6

Choosang, P., & Vasupongayya, S. (2015, 23-26 Nov. 2015). *Using fingerprints to identify personal health record users in an emergency situation.* Paper presented at the 2015 International Computer Science and Engineering Conference (ICSEC).

Darnasser, M. (2013). *Toward privacy-preserving emergency access in EHR systems with data auditing.* (PhD). Rochester Institute of Technology, Retrieved from https://scholarworks.rit.edu/theses/4763

Eikey, E. V., Murphy, A. R., Reddy, M. C., & Xu, H. (2015). Designing for privacy management in hospitals: Understanding the gap between user activities and IT staff's understandings. *Int J Med Inform, 84*(12), 1065-1075. doi:10.1016/j.ijmedinf.2015.09.006

Enaizan, O., Zaidan, A. A., Alwi, N. H. M., Zaidan, B. B., Alsalem, M. A., Albahri, O. S., & Albahri, A. S. (2020). Electronic medical record systems: decision support examination framework for individual, security and privacy concerns using multi-perspective analysis. *Health and Technology, 10*(3), 795-822. doi:10.1007/s12553-018-0278-7

Gardner, R. W., Garera, S., Pagano, M. W., Green, M., & Rubin, A. D. (2009). *Securing medical records on smart phones*. Paper presented at the Proceedings of the first ACM workshop on Security and privacy in medical and home-care systems, Chicago, Illinois, USA. https://doi.org/10.1145/1655084.1655090

Ierache, J., Mangiarua, N., Verdicchio, N., Sanz, D., Montalvo, C., Petrolo, F., & Igarza, S. (2016, 30 Nov.-2 Dec. 2016). *Augmented card system based on knowledge for medical emergency assistance.* Paper presented at the IEEE CACIDI 2016 - IEEE Conference on Computer Sciences.

Jayanthy, S., Anishkka, J. B., Deepthi, A., & Janani, E. (2019, 15-17 May 2019). *Facial Recognition And Verification System For Accessing Patient Health Records.* Paper presented at the 2019 International Conference on Intelligent Computing and Control Systems (ICCS).

Karthikeyan, N., & Sukanesh, R. (2012). Cloud based emergency health care information service in India. *J Med Syst, 36*(6), 4031-4036. doi:10.1007/s10916-012-9875-6

Khan, M. F. F., & Sakamura, K. (2016, 31 Jan.-3 Feb. 2016). *A secure and flexible e-Health access control system with provisions for emergency access overrides and delegation of*

access privileges. Paper presented at the 2016 18th International Conference on Advanced Communication Technology (ICACT).

King, J. T., Smith, B., & Williams, L. (2012). *Modifying without a trace: general audit guidelines are inadequate for open-source electronic health record audit mechanisms*. Paper presented at the Proceedings of the 2nd ACM SIGHIT International Health Informatics Symposium, Miami, Florida, USA. https://doi.org/10.1145/2110363.2110399

Oliveira, M. T. d., Michalas, A., Groot, A. E. D., Marquering, H. A., & Olabarriaga, S. D. (2019, 14-16 Oct. 2019). *Red Alert: Break-Glass Protocol to Access Encrypted Medical Records in the Cloud.* Paper presented at the 2019 IEEE International Conference on E-health Networking, Application & Services (HealthCom).

Orosz, J., Bailey, M., Udy, A., Pilcher, D., Bellomo, R., & Jones, D. (2020). Unplanned ICU Admission From Hospital Wards After Rapid Response Team Review in Australia and New Zealand. *Critical care medicine, 48*(7), e550-e556. doi:10.1097/ccm.0000000000004353

Rothstein, M. (2012). *Access to Sensitive Information in Segmented Electronic Health Records*.

Sandamal, T., Fernando, N., Jayasinghe, I., Xavier, J., Kuruwitaarachchi, N., & Rupasinghe, L. (2019, 5-7 Dec. 2019). *Emergency Patient Identification System.* Paper presented at the 2019 International Conference on Advancements in Computing (ICAC).

Sethia, D., Gupta, D., Mittal, T., Arora, U., & Saran, H. (2014, 6-10 Jan. 2014). *NFC based secure mobile healthcare system.* Paper presented at the 2014 Sixth International Conference on Communication Systems and Networks (COMSNETS).

Sicuranza, M., & Esposito, A. (2013, 9-12 Dec. 2013). *An access control model for easy management of patient privacy in EHR systems.* Paper presented at the 8th International Conference for Internet Technology and Secured Transactions (ICITST-2013).

Sun, J., Zhu, X., Zhang, C., & Fang, Y. (2011, 20-24 June 2011). *HCPP: Cryptography Based Secure EHR System for Patient Privacy and Emergency Healthcare*. Paper presented at the 2011 31st International Conference on Distributed Computing Systems.

Tavares, J., & Oliveira, T. (2016). Electronic Health Record Patient Portal Adoption by Health Care Consumers: An Acceptance Model and Survey. *J Med Internet Res, 18*(3), e49. doi:10.2196/jmir.5069

Thummavet, P., & Vasupongayya, S. (2013, 4-6 Sept. 2013). *A novel personal health record system for handling emergency situations.* Paper presented at the 2013 International Computer Science and Engineering Conference (ICSEC).

Wickramage, C., Fidge, C., Sahama, T., & Wong, R. (2017, 4-8 Dec. 2017). *Challenges for Log Based Detection of Privacy Violations during Healthcare Emergencies.* Paper presented at the GLOBECOM 2017 - 2017 IEEE Global Communications Conference.

Zhang, N., Zang, Y.-L., & Tian, J. (2015). The integration of biometrics and cryptography—a new solution for secure identity authentication. *Journal of Cryptologic Research, 2*(2), 159-176.