A National Minimum Health Log Standard; SAMILOG

Filiz İŞLEYEN[1], Mustafa Mahir ÜLGÜ[2], Kemal Hakan GÜLKESEN[3]

Corresponding Author
Filiz İŞLEYEN

DOI
https:// 10.48121/jihsam.1355992
Received
06.09.2023
Accepted
30.01.2024
Published Online
30.04.2024

Key Words
Computer security, health information systems, privacy, electronic health records

ABSTRACT

Aim: Health data is considered to be highly sensitive and the protection of health data is an ethical and legal responsibility for all health data managing structures. Healthcare organizations use various security measures and techniques to adopt a secure electronic health data recording system in which, in addition, they keep log data. Hospital Information System (HIS) developers had been keeping the log records according to their needs by making the necessary coding for the "change-delete" triggers. Therefore, there was a dire need to develop a common standard for keeping diaries in health information systems. This new standard was considered to be a guide for software developers and was named as Minimum Log Standards in Health (SAMILOG). This study explains the development process of SAMILOG. Method: Focus group meetings were held with seven developer companies. Several scenarios of unauthorized access or data breaches in a health information system were created. The participants discussed each scenario and they evaluated the best methods for keeping logs and which data should be kept as log in each case. Previously, a standard called Minimum Data Model- Minimum Veri Modeli (VEM) was developed to assist data migration to a new HIS software when the hospital administration decides to go for a change. The data field names of VEM standard were also used in this new SAMILOG standard. Results: In SAMILOG 1.0, which of the data elements in each VEM set should be logged was determined, it required an update for SAMILOG as the VEM was updated. Conclusion: SAMILOG v1.0 was announced in 2016 and since then in case of a security breach of health data of public hospitals in Turkey, it is primarily the data logged within the scope of SAMILOG which is examined.

[1] Dr., General Directorate of Health Information Systems, Ministry of Health, Ankara. filiz.isleyen@gmail.com
Orcid Number: https://orcid.org/0000-0002-1277-5757

[2] Assoc. Prof., General Directorate of Health Information Systems, Ministry of Health, Ankara. mahirulgu@gmail.com
Orcid Number: https://orcid.org/ 0000-0003-0825-1851

[3] Assoc. Prof. Department of Biostatistics and Medical Informatics, Faculty of Medicine, Akdeniz University, Antalya. hgulkesen@gmail.com
Orcid Number: https://orcid.org/ 0000-0002-2477-2481

1.INTRODUCTION

Health information is seen as being extremely sensitive, and it is both ethically and legally required to be protected. To establish a safe electronic health record system, healthcare institutions use a variety of security strategies and measures. It is necessary to keep track of all details relating to e-health data including generation time, owner, access records, and usage history (manipulation, update). Accountability can be achieved by locating the person in charge when security incidents happen using recorded data (i.e., an audit trail) (Oh et al., 2021). Log data gives the chance to identify the offender who misused patient data and, in certain cases, results in the professional being disciplined (Kuo et al., 2021). However, a major issue is that health information systems sometimes lack the data required to identify infractions (Malin & Airoldi, 2007). Healthcare is a complex field that includes the possibility of human error (Sameera et al., 2021). Keeping a log ensures that transactions and decisions are traceable. This makes it possible to quickly detect and fix errors. For example, when an incorrect dose of medication is administered or a test result is misinterpreted, logs can help identify the source of these errors. Log records provide a detailed record of events and activities in an information system. Analysis of log records can detect suspicious or malicious activities, identify potential security threats, and provide immediate response to security incidents (Das et al., 2017). Keeping logs in healthcare systems is an essential part of maintaining accurate and comprehensive patient records. These logs serve as a record of all actions taken by healthcare professionals and the systems used in patient care. Healthcare systems must comply with various legal requirements and regulations. Accurate logs can provide evidence of compliance with these requirements and regulations, protecting healthcare organizations from legal and financial liabilities.

Turkey, as a candidate for European Union (EU) membership, has committed itself to harmonizing its domestic law with EU rules and regulations. While working on the draft of Law No. 6698 (Personal Data Protection Law), (Resmi Gazete, 2016) which was published in 2016, the Turkish legislator was inspired by the principles and rules set out in The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 108) and specifically the Data Protection Directive 95/46 (European Union, 1995), which is superseded by the General Data Protection Regulation. Additionally, the Personal Health Data Regulation (Resmi Gazete, 2019) was published in 2019. Because of this legal framework, health information systems are expected to keep a log of user transactions. It is known that logging of health data is a critical element to ensure the security of this data and to protect against unauthorized access. Information such as which user accessed which data and when is important for data security, and logs make it easier to detect such situations. However, there are over 300 companies producing health information systems. There was no standard for keeping logs of health data in Turkey back then. HIS developers kept the log records according to their needs by making the necessary coding for the "change-delete" triggers. Every developer can interpret the need to keep a log according to their subjective point of view. For example, a log can record the activities made through the interface or database. In cases where interface activities are recorded, direct transactions on the database are not recorded. Therefore, the need to develop a common standard for keeping diaries in health information systems was felt. This standard was considered a guide for software producers, and it was expected to constitute a legal basis for future legal problems. This standard was named SAMILOG (Minimum Log Standards in Health). The purpose of this study is to explain the development process of the SAMILOG standard and to provide technical information about the standard.

2. MATERIALS AND METHOD

The development of SAMILOG was the idea of the Ministry of Health (MoH), but the users of this standard are health information system developers. It was decided to work with developer companies, with the help of the data collected through focus group interviews. In Turkey, the MoH determines the standards for HIS software and controls software for compliance with these standards. Additionally, the MoH lists HIS software that conforms to their standards on a website, and only these software companies can provide services in healthcare facilities in Turkey.

SAMILOG is a national level standard study developed to solve two problems. Firstly, which health data should be logged and secondly what method log records should be kept. SAMILOG development studies started in 2015. To determine the participants of the focus group study, health information software companies were contacted, the SAMILOG study was explained, and they were asked whether they would like to participate in the study. Since the ideal number of focus groups is suggested to be between five and eight (Krueger & Casey 2015), seven of the software companies registered on the MoH website were found suitable for our study. These seven software companies, selected according to our records, were serving in 80% of the hospitals in Turkey, and they voluntarily participated in the study. All participants were data migration specialists who had previously participated in the Minimum Data Model (VEM, Minimum Veri Modeli) study. The SAMILOG

standard specifies the name of the data to be logged and does not specify which standard is used. It defines the format of logging, and it is not about the communication standard of log file.VEM is a model developed by the MoH to be used as a standard for data transfers to be made in hospitals in Turkey during hospital information system vendor changes (Isleyen & Ulgu 2020). In this model, a minimum dataset and data model were determined. It is obligatory for every HIS software in in Turkey to be able to create views according to this model from their own databases. For software developers to be "successful" in the audits conducted by the MoH, they must create views from their own databases according to the VEM model.

Several scenarios of unauthorized access or data breaches in a health information system were created. The participants discussed each scenario and evaluated the best methods for keeping logs in each case. Some of the scenarios involved identifying data that should be logged and were based on the experiences of the participants. For example, according to the scenario of one of the participants, within the scope of a legal event, the judicial authorities gave a certain date range and wanted to learn the procedure information applied to the patient in the patient's health records. In SAMILOG, the diagnostic codes of the patients are important, and the activities in the health information systems related to these codes must be logged. Additionally, it has been decided to include the doctor's notes about the patient or the data of the procedures applied to the patient within the scope of SAMILOG. Thus, in the event of any change in these data, it will be known through log records. One of the important questions in the focus group meetings was, "Should log operations be handled and recorded over the application or at the database level". We held four meetings until a consensus was reached. At the end of the meetings, the group decided to keep the log at the database level, in a separate database from the health information system, and they determined the required data components of the log. The draft standard created with the focus group was sent to all companies registered on the MoH website for review. The results of these meetings and the reviews were converted to an official standard, and SAMILOG v1.0 was announced in 2016.

Within the scope of SAMILOG 1.0, only the logs of modifications and deletions were kept. However, it was thought that it was necessary to keep log records in order to add and display data in the retrospective examination processes. For this reason, re-meetings were held with software companies in Turkey, and two sounding questions were determined for SAMILOG 1.1. The first one is, "Should a log be kept for the process of adding and viewing the data?" The second is, "Should the log record be kept in a single table?" Studies on this subject are ongoing, and there is no consensus on the answers to the questions yet.

3. RESULTS

SAMILOG v1.0 is accessible on the web and used by software companies in Turkey (https://sbsgm.saglik.gov.tr/Eklenti/5879/0/samilog-v-10pdf.pdf?_tag1=1250F269EB27F39B914480BEBE1C74A761793DA5). The details of the required data fields are presented in Table I and II.

As of August 2023, there were 205 health information software companies in Turkey. These software companies use various database systems, architectures, and programming languages. Although similar data are kept for each information system, the names given to data fields may be different. Previously, a standard called VEM was developed to assist data migration, when Hospital Information System (HIS) software of a hospital changes. The data field names of VEM standard were also used in this new standard.

Table 1. Log in data that will be kept in the log

Log-in data	
OTURUM_KODU	Session code
KULLANICI_KODU	User code
OTURUM_ACMA ZAMANI	Time of log-in
TERMINAL_ADI	Client name
IP_ADRESI	IP address
MAC_ADRESI	MAC address
UYGULAMA_TURU	Type of application (mobile, web, exe etc.)

Table 2. Update data that will be kept in the log.

Update data	
OTURUM_KODU	Session code
LOG_TABLO_ADI	Table name
LOG_ISLEM_TURU	Transaction type: View (0), Update (1), Delete (2)
ALAN_ADI	Column name (if transaction is 1 or 2)
ESKI_DEGER	Old value (if transaction is 1)
YENI_DEGER	New value (in JSON format) (if transaction is 1 or 3)
SILINEN_KAYIT	Deleted record (in JSON format) (if transaction is 2)
ISLEM_ZAMANI	Time of transaction

In SAMILOG 1.0, it was defined which of the data elements in each VEM set should be logged, and it required an update for SAMILOG as the VEM was updated. VEM sets named in the Table 3, include health data such as patient information, diagnosis and treatment information, medication information and financial information such as invoices issued for transactions applied to the patient.

The Turkish Ministry of Health has a unit that tests and accredits health information systems. The

accredited health information systems are published on our web page, https://kayittescil.saglik.gov.tr/. All currently accredited health information systems must have the ISO 27001 Information Security Management System standard and comply with SAMILOG standards. This international standard has been prepared to provide requirements for the establishment, implementation, maintenance, and continuous improvement of an information security management system (ISO, 2013). All of the currently accredited health information systems comply with SAMILOG standards. Non-accredited health information systems have a very low chance of being marketed in Turkey.

Table 3. Names of the VEM sets.

Names of the VEM sets		
VEM_SURGERY	VEM_PATIENT	VEM_ BOARD_PHYSICIAN
VEM_ SURGERY_TEAM	VEM_PATIENT_ARCHIVE	VEM_ BOARD_REPORT
VEM_SURGERY _PROCESS	VEM_PATIENT_APPLICATION	VEM_REIMBURSEMENT_TRACKING
VEM_ANTIBIOTIC_RESULT	VEM_PATIENT_DENTAL	VEM_PATHOLOGY
VEM_BACTERIAL_RESULT	VEM_PATIENT_EPICRISIS_INFORMATION	VEM_STAFF
VEM_APPLICATION_DIAGNOSIS	VEM_PATIENT_PROCEDURES	VEM_ STAFF_ PAYROLL
VEM_ BUILDING_INFORMATION	VEM_PATIENT_COMMUNICATION	VEM_PERSONEL_PERMISSION_ INFO
VEM_UNIT	VEM_PATIENT_SUPPLIES	VEM_RADIOLOGY_SAMPLE
VEM_DEVICE	VEM_PATIENT_DEATH_ INFORMATION	VEM_ RADIOLOGY_RESULTS
VEM_ WAREHOUSE	VEM_PATIENT_DISPATCH_ INFORMATION	VEM_APPOINTMENT
VEM_DENTAL_ PROSTHESIS	VEM_ PROCEDURES	VEM_PRESCRIPTION
VEM_DENTAL_ PROSTHESIS_DETAIL	VEM_BLOOD_DONOR_ INFORMATION	VEM_PRESCRIPTION_MEDICINES
VEM_DENTAL_ COMMITMENT	VEM_BLOOD_EXIT_ INFORMATION	VEM_ REFERENCE_CODE
VEM_DENTAL_ COMMITMENT_ DETAIL	VEM_ BLOOD_STOCK	VEM_STERILIZATION
VEM_BIRTH	VEM_BLOOD_REQUEST_ INFORMATION	VEM_STOCK
VEM_ BIRTH_DETAIL	VEM_BOARD_ACTIVEINGREDIENT	VEM_EXAMINATION
VEM_ADDITIONAL PAYMENT	VEM_ BLOOD_ PRODUCT	VEM_EXAMINATION_DEVICE_ MATCH
VEM_ADDITIONAL_PAYMENT_ DETAIL	VEM_BLOOD_PRODUCT_ DISPOSAL	VEM_EXAMINATION _SAMPLE
VEM_ADDITIONAL	VEM_CONSULTATION	VEM_EXAMINATION_PARAMETER
PAYMENT_PERIOT		
VEM_INVOICE	VEM_USER	VEM_EXAMINATION_RESULTS
VEM_INVOICE_ DETAIL	VEM_BOARD_DIAGNOSIS	VEM_BED
VEM_FIRM	VEM_USER_GROUP	VEM_CURRENT _INPATIENT
VEM_ BOARD	VEM_GROUP_ MEMBERSHIP	VEM_STAFF_OFFDAYS_STATUS

4. DISCUSSION

In Turkey, at all stages of health service delivery, patient and treatment data is processed and recorded through health information systems used by healthcare institutions, and the MoH centrally regulates these systems. The authorization mechanisms in health information systems may be sufficient for the security of some records, but more effective measures should be taken for sensitive data such as health data. In other words, simply blocking access to data may not be sufficient for its security. When health data is accessed in some way, keeping log records of this access may not be the first access, but it can be a useful method to prevent subsequent accesses. The inadequacy of authorization mechanisms in information systems can be supplemented with log functions (Ross, 2018). While log files were originally used to record information for debugging and diagnostic purposes, they have evolved into recording events and information that is useful for audit trials and forensics in the event of malicious activities or system attacks.

Health data is within the scope of special categories of personal data (Resmi Gazete, 2016; European Union, 1995). Many studies have been carried out on the confidentiality and privacy of this data (Gostin et al., 2009; Moore et al., 2007; Tariq & Hackert, 2018). However, we have not found a study that we can accept as a standard regarding which health data should be more confidential or how access records to these data should be kept. For this reason, we have determined the health records that need to be kept nationally, and standardized them with SAMILOG. Although the scope of SAMILOG is wide, it can be said that it covers all data from a patient's entrance to a health facility until his exit.

Within the scope of ethical and legal requirements, measures should be taken to ensure the security of health data. The fact that a health information system uses a firewall, an antivirus program, or meets the 27001 Information Security Management System Standard does not always mean that health data is safe and cannot be accessed by unauthorized persons. There may also be situations where health data should also be protected from the users of the system, and even though keeping a log record for changing, deleting, or viewing the data does not prevent misuse of health data, it can be a deterrent. Log management in information security

is very important for monitoring and recording user activities, which may be the weakest link in security. The integrity, accessibility, and confidentiality of the data can be ensured by monitoring the operations performed on the data to prevent information leaks and security breaches, which can occur consciously and often unconsciously. Leaving log requirements to hospitals or information system developers without determining the standards would result in keeping logs of different data in every hospital or every health information software. Although health information software (systems) in in Turkey have the 27001 Information Security Management System Standard implemented, SAMILOG has been developed with the need for a common language for such software and has been used since 2016. In case of any security breach, SAMILOG records are first examined by the hospital authorities.

Developing logging standards for health data is also a requirement for the international community. However, SAMILOG is based on VEM, and the international community has not developed a widely accepted database standard for hospital information systems. We hope that our national standards will be an inspiration for developing HIS and health logging standards at the international level. The importance of the SAMILOG study is not only to determine the method for keeping log records but also to be the first study on which health data log records should be kept. Although there are many studies on how to keep log records, there is no study on health data that needs to be logged at the national level. SAMILOG is a standardization study developed for Turkey. VEM was developed to determine the data to be transferred between HIS. SAMILOG, on the other hand, is a standard study that answers the question of which of these data should be logged and technically includes the method for this.

A limitation of SAMILOG is its dependence on another national standard, VEM. As VEM sets are updated, SAMILOG should also be updated. To eliminate this dependency situation and improve SAMILOG, it is considered necessary to carry out additional workshops with software developers.

Conflict of Interest:
The authors declare that they have no known competing financial interests.
Ethical Approval:
There is no need for ethics committee approval, since no studies have been made with human or animal subjects.
Funding:
There is no funding support.
Acknowledgments:
No

REFERENCES

European Union, Directive 95/46/EC of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data. (1995). Available at: https://www.refworld.org/docid/3ddcc1c74.html Accessed 16 May 2023.

Das, R., Baykara, M., & Tuna, G. (2017). Cryptolog: A new approach to provide log security for digital forensics. IU-Journal of Electrical & Electronics Engineering, 17(2), 3453-3462.

Gostin, L. O., Levit, L. A., & Nass, S. J. (Eds.). (2009). Beyond the HIPAA privacy rule: enhancing privacy, improving health through research.

Isleyen, F., & Ulgu, M. M. (2020). Data Transfer Model for HIS and Developers Opinions in Turkey. In Digital Personalized Health and Medicine (pp. 557-561). IOS Press.

Li, G., Hart, A. ve Gregory, J., (1998). Flocculation and sedimentation of high turbidity water, Water Resources, 25, 9, 1137-1143.

ISO. (2013). ISO/IEC 27001:2013(en) Information technology — Security techniques — Information security management systems — Requirements. Last accessed: 09 28, 2022 https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en.

Kişisel Verilerin Korunması Kanunu (2016). Resmi Gazete (Sayı: 29677) https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=6698&MevzuatTur=1&MevzuatTertip=5. Accessed on 23rd Jan 2022.

Kişisel Sağlık Verileri Hakkında Yönetmelik. (2019). Resmi Gazete (Sayı: 30808) https://www.resmigazete.gov.tr/eskiler/2019/06/20190621-3.htm Accessed on 23rd Jan 2022.

Krueger, R.A. & Casey, M.A. (2015) Focus Groups: A Practical Guide for Applied Research. 5th Ed. Thousand Oakes: Sage Publications.

Kuo, K. M., Talley, P. C., & Lin, D. Y. M. (2021). Hospital Staff's Adherence to Information Security Policy: A Quest for the Antecedents of Deterrence Variables. INQUIRY: The Journal of Health Care Organization, Provision, and Financing, 58, 00469580211029599.

Malin, B., & Airoldi, E. (2007). Confidentiality preserving audits of electronic medical record access. Studies in health technology and informatics, 129(1), 320.

Moore, I. N., Snyder, S. L., Miller, C., Qui An, A., Blackford, J. U., Zhou, C., & Hickson, G. B. (2007). Confidentiality and Privacy in Health Care from the Patient's Perspective: Does HIPPA Help?. Health Matrix, 17, 215.

Oh, S. R., Seo, Y. D., Lee, E., & Kim, Y. G. (2021). A comprehensive survey on security and privacy for electronic health data. International Journal of Environmental Research and Public Health, 18(18), 9668.

Ross, R. S. (2018). Risk management framework for information systems and organizations: A system life cycle approach for security and privacy.

Sameera V, Bindra A, Rath GP. Human errors and their prevention in healthcare. J Anaesthesiol Clin Pharmacol. 2021 Jul-Sep;37(3):328-335. doi: 10.4103/joacp.JOACP_364_19. Epub 2021 Oct 12. PMID: 34759539; PMCID: PMC8562433.

Tariq, R. A., & Hackert, P. B. (2018). Patient confidentiality. Available from: https://www.ncbi.nlm.nih.gov/books/NBK519540/