Envisioning the Future of Health Informatics and Digital Health
J. Mantas et al. (Eds.)

doi:10.3233/SHTI250131

Creation of a Unique Patient Identifier Throughout Their Care Journey in Burkina Faso: A Standardized Process

Seydou Golo BARRO[a,b,c,1], Thomas Alassane OUATTARA[a,b,c] and Pascal STACCINI[c]
[a] *Nazi Boni University, Bobo-Dioulasso, Burkina Faso*
[b] *Center for Training and Research in Medical Technology (CFRTM)*
[c] *RETINES/University Côte d'Azur, France*
ORCiD ID: Seydou Golo Barro https://orcid.org/my-orcid?orcid=0000-0001-8274-6700

Abstract. This article describes a process for generating a unique and secure identifier for patients in healthcare institutions, aimed at improving the management of medical data while adhering to security and privacy standards. This process employs data normalization techniques and secure hashing algorithms such as SHA-256, in compliance with international standards such as HL7 for demographic coding and ISO 8601 for dates. The methodology includes key steps: validation of input data, normalization and concatenation of personal information, and application of cryptographic hashes with a random salt. These steps ensure the integrity, authenticity, and compatibility of the identifier with healthcare data management systems. This approach also safeguards patient privacy, preventing tampering and duplication. As such, the process addresses the challenges of security, efficiency, and data standardization in modern healthcare systems, ensuring accurate, unique, and tamper-proof patient identification.

Keywords. Generation process, Anatomopathology, Burkina Faso, Unique identifier, Patients

1. Introduction

In the healthcare field, correct patient identification is crucial to avoid medical errors and improve the efficiency of care services and patient management. The creation of a unique identifier represents an effective solution for centralizing patient information while ensuring its security. This article proposes a method for generating a unique identifier, based on validated identification methods [1] (ref. GMSIH), cryptographic techniques, and international standards such as HL7 for gender coding and ISO 8601 for date formatting. The goal is to create a secure, tamper-proof identifier that is compatible with medical data management systems [2-4].

[1] Seydou Golo BARRO, seydou.barro@gmail.com, +22670468898.

2. Method

The creation of a unique identifier for each patient in Burkinabé healthcare institutions is a crucial step to ensure the security and integrity of medical data. This process is broken down into 11 key steps: 1) The collection and validation of essential personal information about the patient, such as name, first name, gender, date of birth, place of birth, and residence. For example, for a patient named Sanou Ina, the information would be as follows: Name: Sanou, First Name: Ina, Gender: Female, Date of Birth: 08/07/2014, Place of Birth: Bama with code 91006002, Residence: Bobo-Dioulasso with code 91007001. The birth and residence codes are assigned according to the standards of INSD (National Institute of Statistics and Demography) of Burkina Faso, considering the origin and geographical location of the places. 2) Names and first names are normalized, meaning they are transformed to uppercase and concatenated with the "^" symbol, in accordance with the HL7 (Health Level Seven) standard, producing the string "SANOU^INA". 3) To enhance security, a "salt" (random value) is added to this string before performing a hash using the SHA-256 algorithm, generating a unique digital fingerprint, for example:

"27450c3d49e092a9fd3453d96d559e7877bb5ba3e1db8e58ab17f62c73e9e126". 4) Gender is coded according to the HL7 standard: "F" for female, "M" for male, and "U" for unknown. 5) The date of birth is converted to the ISO 8601 format (YYYYMMDD), which results in: "20140708". 6) The birth and residence codes are assigned based on INSD standards to ensure consistency with official systems in Burkina Faso. 7) All these elements (gender, date of birth, initial hash, place of birth, and residence) are concatenated into a complete string:

"F2014070827450c3d49e092a9fd3453d96d559e7877bb5ba3e1db8e58ab17f62c73e9e1269100600291007001". 8) This string is subjected to a second SHA-256 hash, generating a new digital fingerprint, for example:

"d080e41116ddf9eee72a4e9a2f2d0a7ef6259dd863e8d2c039314554683e38da". 9) To facilitate the creation of a unique key, this new fingerprint is converted into an ASCII character sequence, for example:

"10048564810152494949541001001025710110110...". 10) From this sequence, a random 20-character key is generated, for example: "51165557150504418011". Simultaneously, a 2-bit security key is derived from the hash. 11) To create this security key, the last two hexadecimal characters of the hash, for example "da", are converted to decimal, which equals 218. The remainder of the division of 218 by 4 (218 mod 4) gives 2, which is "10" in binary. "Unique identifier: 51165557150504418011", "Security key: 10". This rigorous process ensures the creation of a unique, secure patient identifier that complies with HL7 and ISO 8601 standards, thereby strengthening data protection and the integrity of healthcare systems. Through this systematic approach, healthcare institutions can not only improve the quality of care but also ensure secure and efficient management of patient information. The unique identification system will be strengthened in future efforts in two ways: 1) by conducting regular testing to counter emerging threats and implementing updates to ensure compliance with HL7 and ISO 8601 standards; 2) by assessing its impact on the quality of care, particularly in reducing identification errors, while optimizing its performance through constant monitoring and exploring advanced technologies such as quantum cryptography [5-9].

3. Results

We have implemented a system that, through the application of this methodology, generates a unique and secure identifier for each patient. This system ensures precise and reliable identification within healthcare systems. At the end of the process, the identifier is generated and then assigned to the patient, as shown in Figure 1. Each identifier is designed to be robust and fully compatible with existing medical information systems. For example, for patient Ina Sanou, born on July 8, 2014, the generated unique identifier is 51165557150504418011.

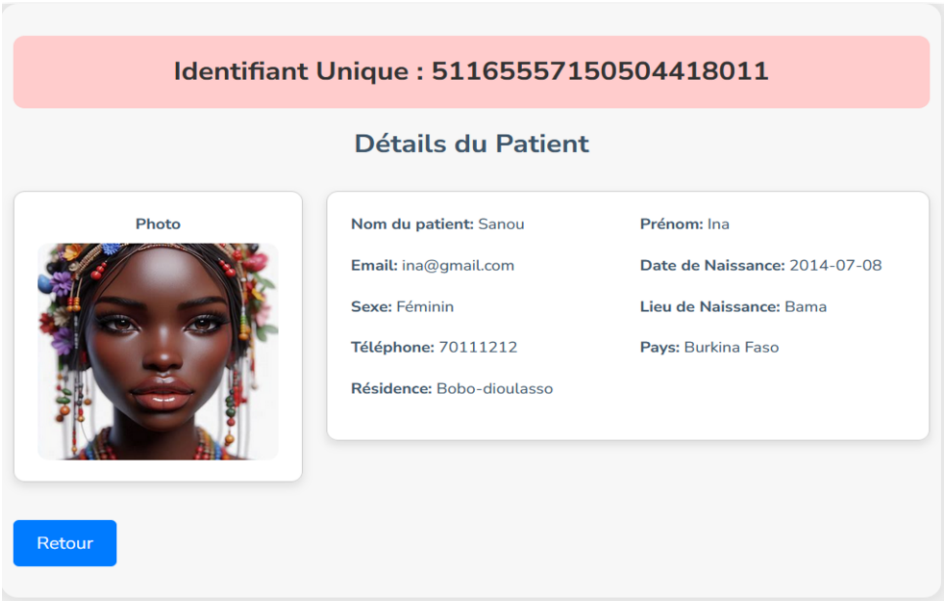

Figure 1. Patient Details Interface

4. Discussion

The unique identifier for patients, created using secure hashing techniques and the addition of a cryptographic salt, represents a significant advancement over traditional identification methods, which are often prone to errors or fraud. By normalizing and concatenating essential patient information (name, date of birth, gender, etc.), this system ensures data uniformity, which is crucial for the integrity of medical records, especially in the context of Burkina Faso, where data management methods vary from one institution to another. Previous studies [10] conducted in the country have attempted to implement patient identification systems but often used SHA-512 as the hashing algorithm. While SHA-512 offers high security, it is often impractical in our context due to its resource requirements and complexity. These studies also did not consider the addition of a random salt, the use of the SHA-256 algorithm, or the application of HL7 and ISO 8601 standards. By neglecting these elements, they left security vulnerabilities that compromise the integrity of patient data. The SHA-256 algorithm proves particularly suitable, as it generates secure hashes while being less resource-intensive than SHA-512,

making it more practical for our context. This system should be applied from the initial patient registration, used during interdepartmental or interinstitutional exchanges, and integrated into electronic medical record management systems. A clear implementation at these key stages ensures its effectiveness in enhancing the security and accuracy of medical data. The addition of a salt for each patient further enhances security, protecting against attacks such as "rainbow tables." Moreover, the adoption of international standards such as HL7 and ISO 8601 ensures compatibility and interoperability with global health systems, facilitating the secure exchange of medical information between institutions. This promotes collaboration between local health structures and global health initiatives, thereby contributing to medical research and telemedicine. However, it is imperative to remain vigilant against technological advancements and emerging threats. Continuous reevaluation of hashing algorithms and cryptographic techniques is essential to maintain a high level of security. This unique identification system not only addresses local challenges in medical data management but also aligns with a global perspective on protecting and enhancing care efficiency. The unique identifier addresses real threats such as cyberattacks (ransomware, data breaches) and identity theft, which compromise the confidentiality and integrity of medical data. This system ensures enhanced traceability and security, which are crucial for protecting sensitive patient information. It should be implemented in hospital databases, national health systems, and international exchanges to ensure secure and standardized management of medical data while reducing errors related to patient identification. This system will enhance data security and reduce errors while aligning with international standards. Efforts will be required for its adaptation in various contexts and raising awareness among users. It will also contribute to significant administrative and clinical benefits in the long term [11-16].

5. Conclusion

The creation of a unique identifier for patients in healthcare institutions is essential to ensure the accuracy of medical records and improve the efficiency of care. By following the steps outlined in this article, it is possible to generate a robust and secure identifier. The use of HL7 and ISO 8601 standards, combined with advanced cryptographic techniques, ensures that this identifier is both standardized and tamper-proof. This process thus contributes to strengthening the management of patient information and improving the quality of healthcare services. The unique identification system will enhance security, quality of care, and the efficiency of the healthcare system. Future efforts will focus on strengthening its resilience, alignment with standards, and widespread adoption. This will support the modernization of the Burkinabe healthcare system.

References

[1] GMSIH, « Identification du patient : Guide pour l'élaboration des politiques d'identification et de rapprochement ». 2000.

[2] Trombert-Paviot B, Couris C-M, Couray-Targe S, Rodrigues J-M, Colin C, Schott A-M. Qualité et utilité d'un identifiant patient anonyme et unique pour le chaînage des séjours hospitaliers dans les bases de données médicoéconomiques françaises. Revue d'Épidémiologie et de Santé Publique. 2007;55:203–211, doi: 10.1016/j.respe.2007.01.029.
[3] Quantin C, Coatrieux G, Fassa M, Breton V, Vlieger P de, Bourquard K, Lipszyc N, Boire J-Y, Roux C, Allaert F-A. Gestion décentralisée des documents médicaux des patients:Un système de recherche et d'accès aux données. Document numérique. 2009;12:23–35.
[4] 54_2.pdf [Internet]. [cited 2024 Sep 24]. Available from: https://repository.oceanbestpractices.org/bitstream/handle/11329/217/54_2.pdf?sequence=1.
[5] AlQudah AA, Al-Emran M, Shaalan K. Medical data integration using HL7 standards for patient's early identification. PLOS ONE. 2021;16:e0262067. doi: 10.1371/journal.pone.0262067.
[6] Synchronization of Health Informatics with "AADHAAR" (UID: Unique Identification) | SpringerLink [Internet]. [cited 2024 Sep 24]. Available from: https://link.springer.com/chapter/10.1007/978-3-642-32573-1_34.
[7] Abdourahamane Diallo. « Interopérabilité des systèmes d'information en santé : Etude comparative et spécificités majeures des normes HL7, EHRCom et OpenEHR ». 2020 [cited 2024 Sep 24]; doi: 10.13140/RG.2.2.17993.57447.
[8] Zlodi M. HL7 norma [Internet] [info:eu-repo/semantics/bachelorThesis]. University of Applied Health Sciences; 2017 [cited 2024 Sep 24]. Available from: https://urn.nsk.hr/urn:nbn:hr:139:045735.
[9] Klyne G, Newman C. RFC3339: Date and Time on the Internet: Timestamps. USA: RFC Editor; 2002.
[10] Golo Barro S, Ugon A, Nana N, R G, Staccini P. Design and Implementation of a Unique Patient Identification Model in Information Systems in Burkina Faso. MEDINFO 2021: One World, One Health – Global Partnership for Digital Innovation [Internet]. IOS Press; 2022 [cited 2024 Sep 24]. p. 238–242. Available from: https://ebooks.iospress.nl/doi/10.3233/SHTI220070.
[11] Anne N, Dunbar MD, Abuna F, Simpson P, Macharia P, Betz B, Cherutich P, Bukusi D, Carey F. Feasibility and acceptability of an iris biometric system for unique patient identification in routine HIV services in Kenya. International Journal of Medical Informatics. 2020;133:104006, doi: 10.1016/j.ijmedinf.2019.104006.
[12] Svandova K, Smutny Z. What Technologies Based on Unique Patient Identifiers Are Used for Patient Identification in Healthcare? In: Mantas J, Hasman A, Demiris G, Saranto K, Marschollek M, Arvanitis TN, Ognjanović I, Benis A, Gallos P, Zoulias E, et al., editors. Studies in Health Technology and Informatics [Internet]. IOS Press; 2024 [cited 2024 Sep 24]. Available from: https://ebooks.iospress.nl/doi/10.3233/SHTI240642.
[13] MORICE Y, MOREL Y. Systèmes d'information. Le GIP GMSIH et la normalisation des systèmes d'information en France. Rev hosp Fr (Paris). 2000;33–39.
[14] Bagayoko CO, Dufour J-C, Avillach P, Quantin C, Fieschi M. Réflexions sur l'identification du patient dans les systèmes d'information de santé. IRBM. 2008;29:302–309. doi: 10.1016/j.rbmret.2008.04.002.
[15] Beale NJ, Rajwany N. Implementation of a unique nurse identifier. Nursing Management. 2022;53:6. doi: 10.1097/01.NUMA.0000805040.87004.37.
[16] An Analysis of Database Management Systems in Mitigating Patient Misidentification Through Unique Patient Identifiers - ProQuest [Internet]. [cited 2024 Sep 24]. Available from: https://www.proquest.com/openview/02b6ba5c87a29cdd38bc1c472c0c6eca/1?pq-origsite=gscholar&cbl=18750&diss=y.