Human Interaction and Emerging Technologies (IHIET-AI 2025), Vol. 161, 2025, 398–407
https://doi.org/10.54941/ahfe1005932

Certificates and the Security of Digital Health Information

Christoph Jungbauer and Christian Luidold

University of Vienna, Multimedia Information Systems, 1090 Vienna, Austria

ABSTRACT

The digitization of healthcare information has expanded access to medical data while raising concerns about its security, authenticity, and trustworthiness. This paper explores the role of digital certificates in addressing these challenges, focusing on their potential to verify the credibility of health information and protect sensitive data. It begins with a theoretical overview, emphasizing the importance of certificates in ensuring data authenticity and integrity, particularly in compliance with regulations such as the GDPR. The analysis examines current certificate models like HONcode and PIF TICK, highlighting their limitations in public awareness and practical application. Innovative technologies such as blockchain and zero-knowledge proofs are identified as promising tools for enhancing the security and traceability of health information. Blockchain's immutability and decentralized verification capabilities, combined with patient-controlled data access via smart contracts, underscore its potential in fostering trust and compliance with privacy standards. The paper outlines essential certification requirements, including technical efficiency through machine learning, content accuracy based on scientific validation, and process transparency. Furthermore, user-centric approaches are emphasized to enhance certificate accessibility and public trust. The study also examines parallels in other industries, such as food and finance, which employ rigorous certification systems for safety and reliability. Ultimately, this research advocates for a hybrid certification model combining automated and expert-driven processes. By leveraging modern technologies and interdisciplinary practices, such a model can address the dual goals of ensuring high-quality health information and fostering user trust in the digital healthcare landscape.

Keywords: Digital health certification, Data security and trust, Blockchain in healthcare

INTRODUCTION

Increasing digitization has greatly expanded the range of health information on the Internet. This development brings both opportunities and challenges, especially with regard to the trustworthiness and security of the information provided (Tarquinio et al., 2021). Many users have difficulty recognizing whether information is scientifically sound and free of economic interests. Certificates can play a central role by guaranteeing the quality and security of digital health information (Boyer et al., 1998). This paper deals with the question of how certificates can contribute to ensuring the authenticity and security of health information. The focus of the investigation is on the aspects of information security.

BACKGROUND

Certificates play a central role in the digital world, especially in healthcare, to ensure the authenticity and security of information. These digital certificates serve as trusted proof that the information transmitted comes from a legitimate source and has not been tampered with in transit. This is especially important in the healthcare sector, where sensitive data such as medical records and diagnoses need to be protected from unauthorized access and tampering.

Digital certificates in healthcare not only ensure the security of information, but also its authenticity by ensuring that the information comes from a trusted source and has not been altered. They help to meet the requirements for data protection and security, such as those required by the GDPR and other data protection laws. In addition, digital certificates are issued by reputable certificate authorities (CAs) that follow strict security protocols to verify the identity of applicants (Brands, 2000).

In the healthcare sector, there are special requirements for certificates. They must guarantee not only the authenticity but also the medical accuracy and independence of the information. On the one hand, this includes the verification of medical devices that ensure that they function correctly and do not pose a danger to the patient, which could have life-threatening consequences (Wirth, Gates, and Smith, 2020). But the accuracy of the information on websites is also playing an increasingly important role.

These certificates and associated management are not only a technical requirement, but also critical to meeting regulatory requirements to ensure patient safety.

Security and Trust Models

The Public Key Infrastructure (PKI) model plays a central role in the certification of information, as it uses asymmetric cryptography to ensure the authenticity and integrity of the data. PKI relies on a system of public and private keys to ensure that data is not tampered with during transmission and comes from the right source. This security architecture is supported by Certificate Authorities (CAs), which establish so-called chains of trust to enable reliable verification of authenticity (Nash, Duane, and Joseph, 2001).

This model is particularly important in the healthcare sector, as the security and confidentiality of sensitive data must be ensured, as required by regulators and data protection laws. In addition to technological security, these certifications must also ensure the scientific accuracy and integrity of health information to increase user confidence in the information and the systems involved (Wirth, Gates, and Smith, 2020; Boyer et al., 1998).

Data Security and Data Protection

The processing and storage of health information is subject to strict data protection regulations, in particular in accordance with the European Union's General Data Protection Regulation (GDPR). These rules aim to ensure the protection of personal data, with health data considered to be particularly vulnerable. Digital certificates play a central role here, as they ensure that

the fundamental principles of information security – confidentiality, integrity and availability (CIA triad) – are maintained. Confidentiality means that only authorized persons have access to the sensitive data, integrity ensures that the data is not altered without authorization, and availability guarantees that the data is accessible when needed (Starkbaum and Felt, 2019).

Current State of Research

There are already several initiatives and standards for certifying digital health information that aim to ensure the trustworthiness and security of this information. The HONcode (Health On the Net) was a first attempt at a certificate that focuses on medical websites and aims to ensure that they provide scientifically sound and transparent information (Boyer et al., 1998). In the UK, there is a similar certification system, the "PIF TICK", which aims to label high-quality health information ("PIF TICK", o. J.).

These certificates are based on clearly defined quality criteria that are intended to ensure scientific accuracy, transparency and independence from economic interests. Although they are an important step towards better orientation for users, analyses show that these certificates are often not sufficient to strengthen user trust in the long term. This is partly due to the fact that they are still too little known among the general population and are often perceived as too complex in their application (Eysenbach, 2001; Laversin et al., 2011)

Technical Certification Approaches

In addition to traditional certificate models such as the HONcode, there are new technological approaches that can ensure the authenticity and security of health information. One such approach is the use of blockchain technologies, which, due to their decentralized structure, enable immutable and transparent verification of information.

This technology ensures that health information cannot be manipulated retrospectively and offers a high level of traceability (Mettler, 2016a). Blockchain-based certificates also offer the advantage of ensuring data integrity without the need for a central control body, which increases user trust.

Another innovative model is zero-knowledge proofs (ZKP), which allow information to be verified without the need to disclose sensitive data. ZKP can be used, for example, to confirm the authenticity of health data without having to disclose details about the patient or specific health status. This is particularly valuable in privacy-sensitive areas such as healthcare (Ben-Sasson et al., 2014).

Requirements for a Certification Process

A certification process for digital health information must ensure that the information can be verified in a simple and automated way. Technologies such as machine learning offer great potential to increase the efficiency of these processes. Machine learning makes it possible to recognize patterns in large amounts of data and evaluate them based on predefined criteria

such as quality and trustworthiness. For example, algorithms can check the medical correctness of content by comparing it with existing databases and automatically make recommendations for certification (Yu, Beam, and Kohane, 2018).

In addition, machine learning enables the continuous adaptation and optimization of certification processes. As the amount of data increases, the algorithm can become more precise and identify erroneous information more quickly. This reduces manual effort and ensures greater accuracy in certification (Amann et al., 2020).

However, one of the biggest challenges in implementing machine learning in certification processes is ensuring that the models are transparent and explainable. It must be ensured that the decisions of the algorithm are comprehensible, especially in sensitive areas such as health information, where trust plays a key role (Topol, 2019).

Content Requirements

In addition to the technical aspects, content criteria must also be considered when certifying health information. The essential requirements include the medical accuracy of the information as well as its scientific evidence. All information must be based on reliable and up-to-date scientific studies and verified by experts to ensure that the recommendations and facts are accurate and up to date (Bello et al., 2021).

In addition, the transparency of interests plays an important role. It must be made clear whether and which economic or other interests are behind the health information to disclose potential conflicts of interest. This builds trust with users and ensures that the information provided is independent and unbiased (Heath, 2020). Certification should be based on clear, standardized guidelines that are regularly reviewed and updated to ensure both the quality and trustworthiness of the information in the long term (Boyer et al., 1998).

Process-Oriented Requirements

The institutions that carry out the digital health information certification process must be independent and trustworthy to ensure that there are no conflicts of interest and that the certification is based on objective criteria. They should have proven expertise in the health sector and have a transparent and comprehensible examination structure. Regular audits are crucial to ensure that certified information remains up-to-date and meets changing scientific and regulatory requirements (Heath, 2020).

Continuous verification of the certificates, for example through annual reviews or real-time updates, ensures that the information always complies with the latest standards and best practices. This not only promotes user trust but also contributes to the long-term security and quality of the information provided (Johannesen, Lindøe, and Wiig, 2020). These measures minimize the risk of outdated or erroneous health information that could be potentially harmful (Boyer et al., 1998).

Technical Opportunities and Challenges

The integration of blockchain technology in healthcare, especially to ensure the authenticity and security of health information, offers a wide range of innovative opportunities. Here are some detailed approaches on how blockchain could be used in this area:

Immutability of Data

One of the main strengths of blockchain is its ability to store information immutably. Once data is recorded in a blockchain, it can no longer be manipulated or deleted retrospectively without this being traceable. This feature makes blockchain an ideal tool for storing and managing sensitive health data. Every change is documented in the blockchain and timestamped, which keeps the entire history of the data transparent and auditable (Mettler, 2016b). This provides peace of mind for patients, who can be sure that their medical data has not been tampered with.

Decentralized Verification

In conventional systems, data responsibility usually lies with a central institution, which can make it a single point of failure. Blockchain, on the other hand, enables decentralized verification of health information. This means that no single entity has complete control over the data, which significantly reduces the risk of data manipulation and misuse. Every transaction on the blockchain is verified by a network of nodes, creating a high level of trust and security (Engelhardt, 2017).

Data Protection and Patient Autonomy

Blockchain can give patients control over their own health data. In traditional healthcare systems, doctors or healthcare providers usually have control over the storage and distribution of patient data. However, by using blockchain, patients can decide for themselves who they want to give access to their health information. Using smart contracts – self-executing contracts on the blockchain – they can authorize or revoke access to their data without having to physically share the data (Radanović and Likić, 2018).

Secure Data Transfer and Interoperability

One of the major challenges in healthcare is the secure and smooth transfer of data between different facilities and systems. Blockchain can serve as a platform for the standardized and secure transmission of health information between different actors in the healthcare system, such as between hospitals, insurance companies and research institutions. By using a blockchain-based system, interoperable health platforms could be developed that exchange data in a standardized and secure manner without the need for central databases (Zyskind and Nathan, 2015).

Compliance With Data Protection Guidelines

With the GDPR and other data protection regulations worldwide, healthcare providers are obliged to ensure the protection of patient data. Blockchain offers a way to comply with these regulations through encryption and the possibility of pseudonymized data storage. Blockchain-based solutions can also ensure that only authorized actors have access to health information and that all accesses are documented in a transparent and traceable manner (Mettler, 2016a).

Potential for Research and Data Analysis

A blockchain can also be used to make health data available for research on a large scale without compromising patient privacy. Anonymous or pseudonymized health data could be stored in the blockchain and used for research purposes without the identity of the patients being revealed. For example, blockchain could significantly increase the efficiency of clinical trials and medical research by enabling secure and controlled access to large amounts of data (Azaria et al., 2016).

User-Centered Perspectives

For a certification process to be successful, it is crucial that users can trust and understand the certificates. For certificates to be truly effective, they must be easily accessible and easy to understand for laypeople. Users should be able to understand the meaning and criteria behind a certificate without in-depth technical or medical knowledge (Paolucci and Neto, 2021).

Certificates should also be integrated in such a way that they serve as clear indicators of trust, e.g. by integrating easily recognizable symbols or labels on websites that offer certified information. This helps users see at a glance that the information is verified and trustworthy (Boyer et al., 1998). In addition, explanations of the certificates could be provided directly on the website to help users understand which standards and criteria have been met and why this is relevant to their health decisions (Bello et al., 2021).

Assessment of Provider Sites and Technical Possibilities

A key aspect of the digital health information certification process is the verification and authentication of provider sites to ensure that the information provided is trustworthy and accurate. This verification requires the fulfilment of certain criteria based on national quality standards such as the Quality Criteria for Good Health Information and other standards planned in the DACH region. These standards aim to ensure scientific accuracy, transparency and independence of information (Boyer et al., 1998; Flaherty et al., 2022; Boyer et al., 1998).

To make the certification process efficient, a central platform is often used where providers can upload their data and information. This information is then automatically checked against predefined criteria to ensure that the content meets the requirements. An example of such a system is Picftick, which is used in the UK to certify trustworthy health information and award visible seals of approval (Picftick, 2021).

Automation Potential

One of the central questions in the certification process is to what extent it can be automated to minimize manual effort. By using yes/no fields and predefined criteria, certain aspects of the certification process can be made more efficient. For example, technical requirements such as compliance with security standards or data protection requirements can be checked relatively easily by automated systems (Paolucci and Neto, 2021).

However, there are substantive criteria, in particular the assessment of medical accuracy and scientific evidence, which cannot be checked purely by machine. In such cases, a hybrid solution could make sense, where automated checks are used to check simple or structured data, while human experts remain responsible for reviewing complex content or the quality of the information (Amann et al., 2020). This ensures high efficiency without compromising on the quality of the certification.

Suitable Software Solutions

There are already various software solutions that are successfully used for similar certification processes in other areas, such as the certification of e-commerce platforms or in the financial services sector. These platforms are often based on automated verification mechanisms that evaluate vendor information according to predefined criteria. These principles can also be applied to the healthcare sector (Xu et al., 2019).

A central platform could be developed for the DACH region that makes it possible to record healthcare providers and their information and certify them based on clearly defined quality criteria. Such a platform could integrate automated checks to ensure that information is always up-to-date and trustworthy. Alternatively, it is possible to adapt existing software solutions to meet the specific requirements of the healthcare sector. This could enable cost-efficient and rapid implementation by leveraging already established techniques (Rehmani et al., 2019).

Optimization for SEO and Search Engines

Another important aspect of the certification process is linking to search engines, especially Google. It would be technically possible to integrate the certificate information into a provider's website in such a way that Google's algorithm prioritizes this information. One way is to use structured data such as Schema.org to make the certificates recognizable to the Google crawler. This could lead to certified health information being ranked higher in searches because it is considered more trustworthy (Schultheiß, Häußler, and Lewandowski, 2022).

In addition, Google could query or cross-check the certificates directly from the certificate authorities. Such an integration could ensure that the contents of the certificate are already included in the search algorithm, which creates a direct link between the certificate authority and the evaluation of the website. This would help websites to verify with.

Comparison With Other Industries

It might be worthwhile looking beyond the health sector and exploring examples from other industries to develop effective approaches to health information certification. Particularly in the food industry and the financial sector, sophisticated certification systems are already in use that are geared towards safety and trust.

In the food industry, certificates such as HACCP (Hazard Analysis and Critical Control Points) play a central role in ensuring the safety and quality of products. This system monitors and controls potential risks in the supply chain and could serve as a model for verifying digital health information to ensure it is secure, accurate, and free from tampering (Rapunzel et al., 2009).

In the financial sector, on the other hand, ISO certifications such as ISO 27001 are widely used to verify information security management systems. These systems ensure that financial data is processed and stored securely and could be transferred to the healthcare sector to ensure the security of sensitive health data (But et al., 2016). These proven systems could provide valuable insights into the development of secure certification mechanisms for the healthcare sector, especially in terms of data security and transparency.

RESULT

The increasing digitization in the healthcare sector offers both opportunities and challenges, especially regarding the trustworthiness and security of the information provided. Certificates play a central role in helping users identify reliable digital health information. They ensure not only technical security, but also the quality of the content of the information. Certificates make a significant contribution to ensuring that health information is not only trustworthy, but also independent and scientifically sound (Boyer, 1998).

It is crucial that the certification process meets both technical and content requirements. By using modern technologies such as machine learning and blockchain, these processes can be designed efficiently and continuously optimized. A combination of automated and manual checks provides the ability to ensure high quality standards without compromising efficiency (Mettler, 2016b; Kritzinger, 2017).

In addition, the process should be transparent and accessible to users. Trust can only be built if the certificates are clear and understandable, and the underlying criteria are made comprehensible to laypeople. Working closely with search engines like Google could also help make certified health information more visible and accessible, further increasing user trust (Schultheiß, Häußler, and Lewandowski, 2022).

Comparable industries, such as the food and financial industries, have already developed sophisticated certification mechanisms that can serve as a model for the health sector. These systems place a strong emphasis on data security and transparency, which is crucial in healthcare (But et al., 2016). The use of proven approaches from other industries could therefore promote the further development of secure and reliable certification processes in the healthcare sector.

Finally, it is essential that the certification process is continuously evaluated and further developed to meet the changing requirements in digital healthcare and to ensure high quality and security in the long term.

REFERENCES

Amann, Julia, Alessandro Blasimme, Effy Vayena, Dietmar Frey, Vince I Madai, and Precise4Q Consortium. 2020. "Explainability for artificial intelligence in healthcare: A multidisciplinary perspective". BMC medical informatics and decision making 20:1–9.

Azaria, Asaph, Ariel Ekblaw, Thiago Vieira, and Andrew Lippman. 2016. "Medrec: Using blockchain for medical data access and permission management". In, 25–30. IEEE.

Bello, Aminu, Ben Vandermeer, Natasha Wiebe, Amit X Garg, and Marcello Tonelli. 2021. "Evidence-based decision-making 2: Systematic reviews and meta-analysis". Clinical Epidemiology: Practice and Methods, 405–28.

Ben-Sasson, Eli, Alessandro Chiesa, Eran Tromer, and Madars Virza. 2014. "Scalable Zero Knowledge via Cycles of Elliptic Curves. 276–294".

Boyer, Celia, Mark Selby, J-R Scherrer, and Ron D Appel. 1998. "The health on the net code of conduct for medical and health websites". Computers in biology and medicine 28 (5): 603–10.

Brands, Stefan. 2000. Rethinking public key infrastructures and digital certificates: building in privacy. MIT Press.

Engelhardt, Mark A. 2017. "Hitching healthcare to the chain: An introduction to blockchain technology in the healthcare sector". Technology Innovation Management Review 7 (10).

Eysenbach, Gunther. 2001. "What is e-health?" Journal of medical Internet research 3 (2): e833.

Flaherty, Sarah Jane, Catherine Duggan, Laura O'Connor, Barbara Foley, and Rachel Flynn. 2022. "What influences a person's willingness to share health information for both direct care and uses beyond direct care? Findings from a focus group study in Ireland". HRB Open Research 5.

Johannesen, Dag Tomas Sagen, Preben Hempel Lindøe, and Siri Wiig. 2020. "Certification as support for resilience? Behind the curtains of a certification body—a qualitative study". BMC Health Services Research 20:1–14.

Kritzinger, Wouter Thomas. 2017. "Development of a search engine marketing model using the application of a dual strategy".

Laversin, Sabine, Vincent Baujard, Arnaud Gaudinat, Maria-Ana Simonet, and Célia Boyer. 2011. "Improving the transparency of health information found on the internet through the honcode: a comparative study". In User Centred Networked Health Care, 654–58. IOS Press.

Maarop, Nurazean, Kavitha Thamadharan, Ganthan Narayana Samy, Norziha Megat Mohd Zainuddin, Azri Azmi, Othman Mohd Yusop, and Azizul Azizan. 2016. "Information security management system implementation success factors: A review". Advanced Science Letters 22 (10): 3023–26.

Mettler, Matthias. 2016a. "Blockchain technology in healthcare: The revolution starts here". In, 1–3. IEEE.

———. 2016b. "Blockchain technology in healthcare: The revolution starts here". In, 1–3. IEEE.

Nash, Andrew, William Duane, and Celia Joseph. 2001. PKI: Implementing and Managing E-security. McGraw-Hill, Inc.

Paolucci, Rodolfo, and André Pereira Neto. 2021. "Methods for evaluating the quality of information on health websites: Systematic Review (2001–2014)". Latin American Journal of Development 3 (3): 994–1056.

"PIF TICK". n.d. Accessed October 23, 2024 https://pifonline.org.uk/pif-tick/.

Radanović, Igor, and Robert Likić. 2018. "Opportunities for use of blockchain technology in medicine". Applied health economics and health policy 16:583–90.

Rehmani, Mubashir Husain, Alan Davy, Brendan Jennings, and Chadi Assi. 2019. "Software defined networks-based smart grid communication: A comprehensive survey". IEEE Communications Surveys & Tutorials 21 (3): 2637–70.

Schultheiß, Sebastian, Helena Häußler, and Dirk Lewandowski. 2022. "Does Search Engine Optimization come along with high-quality content? A comparison between optimized and non-optimized health-related web pages". In, 123–34.

Starkbaum, Johannes, and Ulrike Felt. 2019. "Negotiating the reuse of health-data: Research, big data, and the European general data protection regulation". Big Data & Society 6 (2): 2053951719862594.

Rapunzel, Satu, Nina Kaario, Riitta Maijala, Hannu Korkeala, and Anu Tulokas. 2009. "Operators in implementing food law in". Archiv für Lebensmittelhygiene 60 (6): 172–78.

Tarquinio, Camille, Christine Rotonda, Pascale Tarquinio, Fanny Bassan, Marie-Jo Brennstuhl, and Cyril Tarquinio. 2021. "Chapter 63. Therapeutic alliance and evolution towards e-health". In The Therapeutic Alliance, 401–5. Dunod.

Topol, Eric J. 2019. "High-performance medicine: The convergence of human and artificial intelligence". Nature medicine 25 (1): 44–56.

Wirth, Axel, Christopher Gates, and Jason Smith. 2020. Medical Device Cybersecurity for Engineers and Manufacturers. Artech House.

Xu, Yao-Zhi, Jian-Lin Zhang, Ying Hua, and Lin-Yue Wang. 2019. "Dynamic credit risk evaluation method for e-commerce sellers based on a hybrid artificial intelligence model". Sustainability 11 (19): 5521.

Yu, Kun-Hsing, Andrew L Beam, and Isaac S Kohane. 2018. "Artificial intelligence in healthcare". Nature biomedical engineering 2 (10): 719–31.

Zyskind, Guy, and Oz Nathan. 2015. "Decentralizing privacy: Using blockchain to protect personal data". 180–84. IEEE.