


# Security, privacy, and confidentiality in electronic prescribing systems: A review study

Reyhane Norouzi Aval<sup>1</sup>, Seyyedeh Fatemeh Mousavi Baigi<sup>1</sup>, Masoumeh Sarbaz<sup>2</sup>, Khalil Kimiafar<sup>2\*</sup> 

<sup>1</sup>MSc Student of Health Information Technology, Department of Medical Records and Health Information Technology, School of Paramedical Sciences, Mashhad University of Medical Sciences, Mashhad, Iran

<sup>2</sup>Associate Professor, Department of Medical Records and Health Information Technology, School of Paramedical Sciences, Mashhad University of Medical Sciences, Mashhad, Iran

## Article Info

### Article type:

Review

### Article History:

Received: 2022-04-16

Accepted: 2022-05-09

Published: 2022-05-25

### \* Corresponding author:

Khalil Kimiafar

Associate Professor, Department of Medical Records and Health Information Technology, School of Paramedical Sciences, Mashhad University of Medical Sciences, Mashhad, Iran

Email: [Kimiafarkh@muma.ac.ir](mailto:Kimiafarkh@muma.ac.ir)

### Keywords:

Electronic Copywriting

Privacy

Confidentiality

Security

## ABSTRACT

**Introduction:** The use of electronic prescribing has identified as a strategically important policy to improve health care. Therefore, the purpose of this study was to review the issues related to security, privacy and privacy of electronic copying systems.

**Material and Methods:** A comprehensive review of studies were conducted that published in English, free access to the full text of the article and without time limitation, by searching for keywords in keywords, title and abstract of studies in valid scientific databases Web of Science, Scopus, PubMed and Embase in June 4, 2021. Two researchers reviewed the title and content of searched studies independently. 137 related studies found and finally 25 main articles selected.

**Results:** In general, the results of the study showed that in some countries, there are still no minimum requirements and standards for these systems; But the use of security and privacy protocols has been used in various ways. However, according to other studies, most patients and physicians are concerned about the privacy and security of medical data in the context of these systems. In general, security in an electronic healthcare system includes the seven main components of user authentication, patient confidentiality, licensing issues, scalability, integrity, non-denial, and confidentiality of information sent, processed, and stored.

**Conclusion:** In this study, different protocols were classified into 7 main components. Although there are different protocols to ensure security, privacy and confidentiality issues; But the lack of international security requirements poses a major challenge to the adoption of electronic transcription systems. Given that the majority of patients and physicians were concerned about the issues of privacy and security of medical data, it is necessary for policy makers and managers in this area to pay attention to these issues before implementing these systems and provide a safe environment for implementing these systems. Provide patient privacy.

## Cite this paper as:

Norouzi Aval R, Mousavi Baigi SF, Sarbaz M, Kimiafar K. Security, privacy, and confidentiality in electronic prescribing systems: A review study. *Front Health Inform.* 2022; 11: 115. DOI: [10.30699/fhi.v11i1.374](https://doi.org/10.30699/fhi.v11i1.374)

## INTRODUCTION

Electronic prescription (EP) is an emerging technology that replaces handwritten prescriptions and allows healthcare providers (pharmacists, doctors, nurses, and the like) to transfer electronic prescriptions to smart pharmacies [1]. Electronic prescribing systems are key components and drivers of digital health and increase patient safety by

reducing transcription errors [2]. Electronic communication of health care data, including documents such as doctor prescriptions, laboratory research, and counseling, is a growing challenge for health care departments, as it can greatly reduce the complexity of current documentation, providing health care services in a fast and reliable manner. Increase and support health care. However, such an approach carries serious security risks because any

change, exposure to unauthorized persons, or loss of health care information may endanger human life. In this regard, it is necessary to rely on health care data to ensure its accuracy and availability, as this data may be the basis for important decisions about treatment and medication, the confidentiality of personal, medical and administrative information due to social effects. Be moral and psychological [3].

Health care professionals are legally and ethically obliged to protect the confidentiality of patient information [4, 5]. However, systems security can often lead to less use of them. In general, the more secure a system is, the less it is used. Security problems often cause users to worry and not accept systems. In addition, weaknesses in the security infrastructure prevent healthcare providers, including physicians, from using it. On the other hand, very strong security infrastructures lead to time-consuming or non-operational systems, which may make some or all users prefer to continue using the existing paper-based system [4].

Therefore, for electronic copy systems to be successful, a fine balance must be struck between security and accessibility. Therefore, the purpose of this study is to review the issues related to security, privacy and privacy of electronic copying systems.

## MATERIAL AND METHODS

This review study was performed using a systematic search with specific entry and exit criteria. This systematic review by searching the keywords "Electronic Prescribing", E-Prescription, E-prescribing, Confidentiality, privacy and security in the keywords, title and abstract of studies in the valid scientific databases Web of Science, Scopus, PubMed and Embase on June 4, 2021 Was explored.

Studies published in English, free access to the full text of the article and no time constraints when aligned with the purpose of the study were considered as criteria for inclusion in the study and were reviewed separately by two researchers. Exclusion criteria included studies in the form of letters to the editor, conference summaries, lack of access to the full text of articles, as well as irrelevant studies whose purpose was inconsistent with the present study.

After reviewing the articles and removing duplicate articles (65 articles), 72 articles were obtained and their screening was evaluated based on the titles and abstracts of the article. At the end of the review, 29 articles that had nothing to do with the purpose of this study were deleted. Then, 43 articles were selected to review their full text, of which 18 articles were deleted and finally 25 articles were reviewed. Figure 1 shows the steps for selecting studies using the PRISMA chart. In the data extraction phase, the two researchers independently reviewed the

selected articles for the full text. Any differences between the extracted data and the results of the studies will be resolved through discussion and consensus between the parties, and in case of disagreement, the third author will give a final opinion for review.

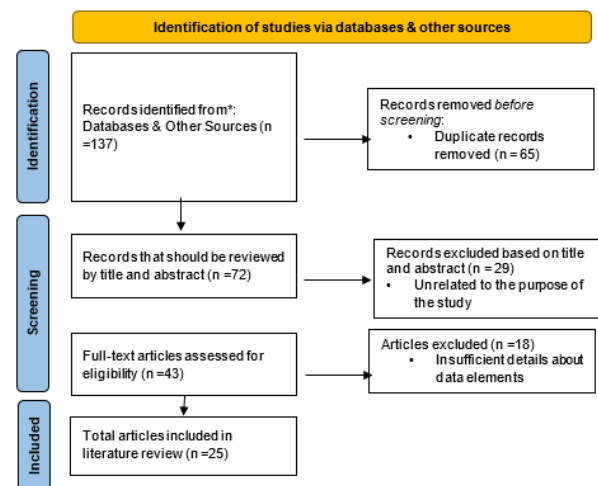


Fig 1: Study selection chart

## RESULTS

The results of the study showed that in some countries there are still no minimum requirements and standards for these systems [2, 4, 6]. However, the use of security and privacy protocols has been used in various ways [3, 7-9]. In general, security in an electronic health care system includes the seven main components of user authentication, patient confidentiality, licensing issues, scalability, integrity, non-denial, and confidentiality of information sent, processed, and stored. Which are as follows:

1. **User authentication:** Anyone using an electronic transcription system must be reliably identified [7, 10]. This is to ensure that only authorized professionals can access the system, and also allows all records and accesses to be accurately recorded and reviewed. The process of reliably identifying authorized individuals can be accomplished using advanced login and password mechanisms or authentication tools such as digital certificates stored on smart cards to assign patient consent (2-9-9), according to a predefined map. Used to access data and authorize users to access system resources [1, 4, 7, 10, 11].
2. **Patient confidentiality:** Confidentiality is to ensure that patient details and prescriptions are not made available to unauthorized individuals, individually or collectively. In the electronic world, data confidentiality can be controlled using a private network with precise and controlled access, or data encryption techniques, or both (by creating unique identities for the patient, physician, and access

persons). If a private network is to be used instead of encryption, it must be ensured that only authorized persons can access the network. All access terminals, computers, cables, and network ports must be in secure physical areas to ensure that unauthorized persons cannot connect to the network. Authorized users should also be trained to ensure that they do not intentionally or mistakenly connect a private network to a public network. Of course, maintaining completely secure private networks is very difficult and must be carefully managed. There is a lot of cost involved in this. Encryption techniques allow confidential data to be transmitted over public networks such as the Internet, provided the encryption mechanism is strong enough to prevent unauthorized disclosure [1, 3, 4, 10, 12, 13].

3. Licensing issues: We need to make sure that only authorized personnel have access to the patient's confidential data, and that they only have access to the data set they need to see. In the world of security, this is known as the principle of minimum score. Use for them or in absolutely necessary cases. When you associate this with electronic transcription, there are two consequences [1, 4]. First, pharmacists should not have access to all the prescriptions prescribed by all GPs; they should only have access to the prescriptions that the patient has requested. Second, when transcripts are transferred between systems, no other authorized professionals should have access to them. This means that copies must be encrypted so that only authorized recipients can decrypt them [6, 10].

4. Scalability: The electronic prescribing system must be available 24 hours a day, 365 days a year, as the patient may need a prescription at any time. This means that every version and distributor must always have access to the EP system under any operating conditions [4]. This can be achieved by building a robust, strong IT infrastructure [6, 7] and using the HL7 [2, 7] protocols.

5. Integration: Integration is the process of ensuring the compatibility of data in the creation, modification or destruction of unauthorized data. This can be done in the same way as a handwritten signature, but with a digital signature mechanism, linking the user uniquely to their digital certificate [4, 15, 16]. Other solutions include developing international data exchange standards (7, 28%) and updating existing security requirements and regulations [6, 10].

6. Non-refutation: The process by which the recipient claims to know the origin of the data so that the sender can later falsely deny sending the data (not rejecting the source) or the process by which the sender claims to send some data. Knows that this data has successfully reached the intended recipient (no receipt). For example, the use of digital signatures and registration, the name of the data registrar in the submitted sources [15, 16].

7. Confidentiality of information sent, processed and stored: It is the process of protecting against information that is disclosed or disclosed for unauthorized purposes. This can be done using cryptographic algorithms and encryption mechanisms using XML-based services [3], both at the application level (with smart card capability for private key storage) and at the network protocol level using secure protocols [10, 12, 13, 17].

## DISCUSSION

Electronic prescribing systems are key components and drivers of digital health and can enhance safety [2]. Given that the success of electronic copywriting systems depends on a delicate balance between security and accessibility. Therefore, the purpose of this study is to review the issues related to security, privacy and privacy of electronic version systems.

The results of the study showed that security in electronic health care system includes 7 main components of user authentication, patient confidentiality, licensing issues, scalability, integrity, non-denial and confidentiality of information sent, processed and stored. Electronic communications of medical records carry some serious security risks, as most patients and physicians in the study have stated that they are concerned about the privacy and security of medical data in the context of these systems [12, 18-22].

Therefore, one of the important principles of achieving user acceptance of electronic prescription systems is to build a strong infrastructure in health care services to ensure that electronic systems do not pose a threat to their information. To achieve this, Bourka et al. Recommend requirements such as access only to authorized persons, physician access only for a specific purpose, encrypted communications, and recording the date and time of data entry [3]. Communications must be guaranteed with security requirements, accuracy, authenticity, non-denial and inflexibility, respectively. One way to achieve this type of security countermeasures when transmitting electronic transcript data is to encrypt. Cryptography is associated with digital signature and encryption in electronic transcription [23].

Smart card technology also offers a ready-made solution to some basic security problems. Smart cards enable personal authentication and secure communications, thus providing a mechanism for strong security, different access to data, and definitive audit trails [8, 24]. Yang et al. Proposed an electronic version system based on the smart card. They considered the issues of privacy and delegation in the electronic version system and used the concept of group signature and proxy signature schemes for presentation [25].

Li et al. Also recognize block chain as a new way to

secure electronic version systems. This technology is for data storage in a secure and distributed manner that requires a centralized reference to control and validate the data [26]. Ullah et al. Also proposed a CB-PS-certified proxy sign encryption scheme in response to the guarantee of confidentiality and authentication to combine both encryption and digital signature functions in the electronic transcription system [10].

One of the strengths of this study was the classification of important security issues and the inclusion of various security protocols in electronic prescription systems, which leads to a deeper understanding of security issues in electronic prescription systems, better acceptance and facilitates the implementation of these systems. Among the limitations of this study, the keywords searched may not be sufficient and complete to obtain further studies, and some prominent and relevant studies may not be included in this study. In addition, only studies published in scientific journals and conference proceedings are included in this study; therefore, it does not cover articles published in the gray literature.

## CONCLUSION

In this study, different protocols were classified into

7 main components. Although there are different protocols to ensure security, privacy and confidentiality issues; but the lack of international security requirements poses a major challenge to the adoption of electronic transcription systems. Given that the majority of patients and physicians were concerned about the issues of privacy and security of medical data, it is necessary for policymakers and managers in this area to pay attention to these issues before implementing these systems and provide a safe environment for implementing these systems. Provide patient privacy.

## AUTHOR'S CONTRIBUTION

All authors contributed to the literature review, design, data collection and analysis, drafting the manuscript, read and approved the final manuscript.

## CONFLICTS OF INTEREST

The authors declare no conflicts of interest regarding the publication of this study.

## FINANCIAL DISCLOSURE

No financial interests related to the material of this manuscript have been declared.

## REFERENCES

- Bhatia T, Verma A. Cryptanalysis and improvement of certificateless proxy signcryption scheme for e-prescription system in mobile cloud computing. *Annals of Telecommunications*. 2017; 72(9): 563-76.
- Aldughayfiq B, Sampalli S. Digital health in physicians' and pharmacists' office: A comparative study of e-prescription systems' architecture and digital security in eight countries. *OMICS*. 2021; 25(2): 102-22. PMID: 32931378 DOI: 10.1089/omi.2020.0085 [PubMed]
- Bourka A, Kaliontzoglou A, Polemi D, Georgoulas A, Sklavos P. Enriching healthcare applications with cryptographic mechanisms and XML-based security services. *Technol Health Care*. 2003; 11(1): 61-76. PMID: 12590159 [PubMed]
- Mundy D, Chadwick DW. Security issues in the electronic transmission of prescriptions. *Med Inform Internet Med*. 2003; 28(4): 253-77. PMID: 14668129 DOI: 10.1080/14639230310001621675 [PubMed]
- Data Protection Act [Internet]. 1998 [cited: 1 Dec 2021]. Available from: <https://www.parliament.uk/globalassets/document/s/foi/Advice-for-Members-and-Data-Protection-Feb15-WEB.pdf>
- Kierkegaard P. E-prescription across Europe. *Health and Technology*. 2013; 3(3): 205-19.
- Gall W, Aly AF, Sojer R, Spahni S, Ammenwerth E. The national e-medication approaches in Germany, Switzerland and Austria: A structured comparison. *Int J Med Inform*. 2016; 93: 14-25. PMID: 27435943 DOI: 10.1016/j.ijmedinf.2016.05.009 [PubMed]
- Hsu CL, Lu CF. A security and privacy preserving e-prescription system based on smart cards. *J Med Syst*. 2012; 36(6): 3637-47. PMID: 22407399 DOI: 10.1007/s10916-012-9838-y [PubMed]
- Hamze M, Peyrard F, Conchon E. An improvement of NFC-SEC with signed exchanges for an e-prescription-based application. In: Memmi G, Blanke U (eds). *Mobile computing, applications, and services. Lecture notes of the institute for computer sciences, social informatics and telecommunications engineering*, vol 130. Springer, Cham; 2014.
- Ullah I, Amin N, Almogren A, Khan MA, Uddin MI, Hua Q. A lightweight and secured certificate-based proxy signcryption (CB-PS) scheme for e-prescription systems. *IEEE Access*. 2020; 8: 199197-212.
- Ross J, Pinkas D, Pope N. Electronic signature policies. RFC 3125, The Internet Society; 2001.
- Steinschaden T, Petersson G, Åstrand B. Physicians' attitudes towards e-prescribing: A comparative web survey in Austria and Sweden. *Inform Prim Care*. 2009; 17(4): 241-8. PMID: 20359402 DOI: 10.14236/jhi.v17i4.743 [PubMed]
- Niinimä J, Savolainen M, Forsström JJ. Methodology for security development of an electronic prescription system. *Proc AMIA Symp*. 1998; 245-9. PMID: 9929219 PMID: PMC2232178 [PubMed]

14. Report on the review of patient-identifiable information [Internet]. 1997 [cited: 1 Dec 2021]. Available from: [http://www.wales.nhs.uk/sites3/documents/950/d\\_h\\_4068404.pdf](http://www.wales.nhs.uk/sites3/documents/950/d_h_4068404.pdf)
15. Blobel B, Bleumer G, Muller A, Flikkenschild E, Ottens F. Current security issues faced by health care establishments. In: The ISHTAR Consortium (ed). *Studies in Health Technology and Informatics*. Vol 66. IOS Press; 2001.
16. Sizer R. Information technology security evaluation criteria. *Computer Bulletin*. 1986; 1993: 5.
17. Porterfield A, Engelbert K, Coustasse A. Electronic prescribing: Improving the efficiency and accuracy of prescribing in the ambulatory care setting. *Perspect Health Inf Manag*. 2014; 11(Spring): 1g. PMID: 24808808 [[PubMed](#)]
18. Schiff G, Seoane-Vazquez E, Wright A. Incorporating indications into medication ordering: Time to enter the age of reason. *N Engl J Med*. 2016; 375(4): 306-9. PMID: 27464201 DOI: 10.1056/NEJMp1603964 [[PubMed](#)]
19. Spil TA, Cellucci LW. Electronic health records across the nations. *Health Policy and Technology*. 2015; 4(2): 89-90.
20. Gider Ö, Ocak S, Top M. Evaluation of electronic prescription implications in Turkey: An investigation of the perceptions of physicians. *Worldviews Evid Based Nurs*. 2015; 12(2): 88-97. PMID: 25773862 DOI: 10.1111/wvn.12082 [[PubMed](#)]
21. Garada M, McLachlan AJ, Schiff GD, Lehnbohm EC. What do Australian consumers, pharmacists and prescribers think about documenting indications on prescriptions and dispensed medicines labels? A qualitative study. *BMC Health Serv Res*. 2017; 17(1): 734. PMID: 29141618 DOI: 10.1186/s12913-017-2704-3 [[PubMed](#)]
22. Lapane KL, Waring ME, Dubé C, Schneider KL. E-prescribing and patient safety: Results from a mixed method study. *Am J Pharm Benefits*. 2011; 3(2): e24-34. PMID: 24179595 [[PubMed](#)]
23. Zheng Y, editor *Digital signcryption or how to achieve cost (signature & encryption) << cost (signature) + cost (encryption)*. Annual International Cryptology Conference. Springer; 1997.
24. Tamizhselvan C, Vijayalakshmi V. An energy efficient secure distributed naming service for IoT. *International Journal of Advanced Studies of Scientific Research*. 2018; 3(8): 1-5.
25. Yang Y, Han X, Bao F, Deng RH. A smart-card-enabled privacy preserving e-prescription system. *IEEE Trans Inf Technol Biomed*. 2004; 8(1): 47-58. PMID: 15055801 DOI: 10.1109/titb.2004.824731 [[PubMed](#)]
26. Li P, Nelson SD, Malin BA, Chen Y. DMMS: A decentralized blockchain ledger for the management of medication histories. *Blockchain Healthc Today*. 2019; 2: 38. PMID: 32524086 DOI: 10.30953/bhty.v2.38 [[PubMed](#)]