Distributed Database Model for Mobile Health Telemonitoring Applications

Paulo Veloso Gomes, Henrique Curado, António Marques, Bárbara Gomes, and Javier Pereira

LabRP, Center for Rehabilitation Research, School of Health, Polytechnic of Porto, Porto, Portugal
CITIC Research Center, University of A Coruña, A Coruña, Spain
Correspondence: velosogomes@ess.ipp.pt

DOI: *https://doi.org/10.17979/spudc.000024.07*

Abstract: Telemonitoring interventions in patients allow to collect and transmit information to health professionals bringing recognized advantages in the personalization of health care services. Those applications deal with sensitive data, raising ethical and legal issues that must be considered. Guarantee the quality and accuracy of the data collected in telemonitoring and ensure confidentiality to protect the patient privacy is a fundamental requirement. The patient's informed consent implies that he is aware of the potential benefits and risks of the system, how telemonitoring will be used, what data will be collected and with whom it will be shared. This work proposes a database model ensuring that sensitive data is handled securely and accessible only to authorized health professionals.

1 Introduction

The evolution of communication and information technologies opens up new opportunities for improving the provision of healthcare. The evolution, portability and dissemination of new devices that allow sophisticated applications and facilitate the communication process through wireless networks, allows the creation of new networks and forms of communication between healthcare professionals, patients and informal caregivers.
The concept of telemonitoring opens new opportunities in the area of healthcare provision. Its application can have different purposes, counseling, monitoring, communication between the user and the healthcare professional, selfcare management, among others.
The development of telemonitoring applications focused on the centralization of care in patients must consider the perspectives of different stakeholders. Despite the advantages that telemonitoring can provide to patients, healthcare professionals and the healthcare system in general, there are also important challenges that must be carefully studied, so as not to compromise the quality of healthcare services provided, patient privacy and the protection of healthcare professionals.
Telemonitoring applications raise some important challenges, such as data protection, confidentiality, reliability, accuracy of information, ensuring that the patient is effectively and properly informed before giving informed consent and that the healthcare professional can prove afterwards that provided a quality service in a timely manner. Studies show that privacy and security are the main concerns of users of this type of systems (Houser et al., 2023), (Pool et al., 2022). Technology constraints and digital literacy are other important challenges mentioned (Houser et al., 2023).
In this work, we seek to propose a database model that guarantees that sensitive data are

treated, at the telemonitoring level, in a secure manner and accessible only to authorized health professionals, it is essential that the privacy and informed consent of the patient is guaranteed, the basis of any intervention. It is important to note that we are in the field of telemonitoring, through mobile applications that are not owned by healthcare providers, when there is already legal support for the collection of data in databases, in accordance with the General Data Protection Regulation (GDPR).

2 Trust, Confidence and Privacy

The doctor-patient relationship is based on trust. This, however, is not unilateral. Not only is it imperative that the patient trusts his doctor and understands the information he gives him, it is also essential that the doctor obtains all the necessary information, without omissions, to know how to advise the person. This double dimension is even more relevant in terms of telemonitoring, as it requires the patient to provide the necessary data in an accurate and timely manner. This presupposes that patients have confidence in the system and the guarantee of confidentiality of their data. On the other hand, it presupposes that the doctor is able to demonstrate that, given the available data, he did everything in terms of providing the best advice in accordance with the Clinical Guidance Standards and his objective duty of care. This scenario falls within the domain of medical, ethical, civil and criminal liability.
It is not intended to analyze issues of medical liability here, as they cannot be dissociated from telemonitoring. Indeed, if an error occurs during the process, this may be due to the doctor, his patient, but also to the mechanism used, as machines, programmed by humans, are also fallible (Lança, 2022). It is clear, therefore, that the health professional must have at his disposal means that allow him to prove his lack of guilt or negligence. However, this is only possible if the healthcare professional has access to their patients' sensitive data, under penalty of, in the face of an accusation, whether founded or not, being unable to obtain elements necessary for his defense.
This dimension rules out the possibility of telemonitoring mechanisms allowing access to health professionals only for a limited period, during which they would make a statement, leaving the database only with the holder of the same, the patient. For this, but also for another reason, which is the need for data analysis to presuppose the perception of clinical history, access to health data in telemonitoring must be complete. This aspect thus falls into the domain of health information security. It should be noted that at this level, not only data protection legislation is relevant, ethical questions also arise.

3 Informed Consent

Informed consent must exist at two levels. At the first level, the patient, when accessing the telemonitoring process, will have to give their consent for sensitive data to be processed (data concerning health, as defined in article 4 of the GDPR, is "personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status"). Thus, consent is in the sense of the GDPR, which presupposes not only collection, but also access, and its transfer and deletion.
On the other hand, when the doctor in the monitoring process provides an intervention, which may constitute a medical act, it is necessary that, in the interests of his/her release from responsibility, he/she is aware that the patient, when carrying out the act (clinical, pharmacological, etc.) has was completely clear about the scope of what was advised. This is another level of consent, which, although normally called informed consent, also consists of a therapeutic clarification (Pereira, 2020), because if it is advised to take or change a drug, the patient will have to be duly informed of possible side effects or adverse reactions.
Finally, the ethical issue must be borne in mind. In effect, the doctor must, when taking on the telemonitoring process, in addition to the ethical obligation of confidentiality, which does not

have any incompatible relationships, namely, by providing services in private groups, or having any financial participation in them, for the which monitored data may have any economic interest, directly or indirectly (which will occur if the doctor works in a clinic owned by a health insurance group).
In the field of monitoring, whether of chronic patients or less complex processes, through electronic devices, usable remotely, making the privacy of health data compatible with the responsibility of the healthcare professional requires a careful and balanced approach. It is essential to prioritize the protection of sensitive patient data while allowing professionals to provide the best care possible. This can be achieved through secure technology in compliance with data privacy and medical liability legislation, through the use of mutual intervention mechanisms: the patient's double consent; the medical assumption of guaranteeing total confidentiality, through the non-consent agreement for third parties to access the information.
Despite its unquestionable contribution to individual and collective health, when dealing with health information, which is highly sensitive, the protection of privacy based on a system that merely refers to the GDPR, does not provide effective protection (Curado et al., 2023). A Distributed Database Model for Mobile Health Telemonitoring Applications (Figure 1) must consider a flexible use of data, ensuring that data is only accessed by those who need it and have the necessary access permission.

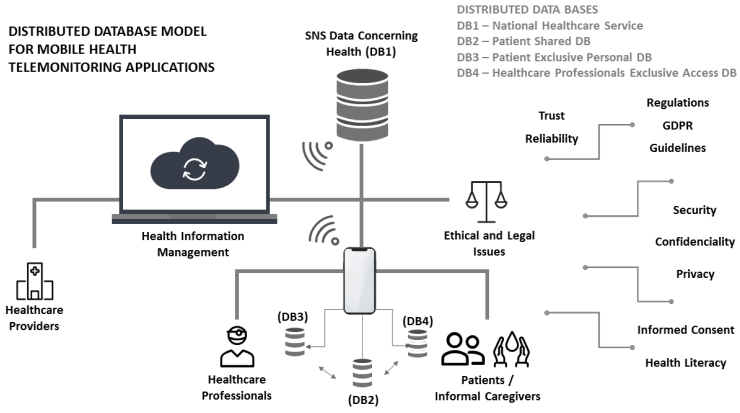

Figure 1: Distributed Database Model for Mobile Health Telemonitoring Applications

Therefore, the proposal to develop a "mobile application that allows users of the National Health Service, who are in Telemonitoring programs, to record measurements of biometric parameters and self-assessments", deserves a more careful analysis of the proposed terms and conditions of use recommended by Shared Services of the Ministry of Health (https://www.spms.min-saude.pt/telemonitorizacao-sns).

4 Conclusion

The new information and communications technologies have triggered a new paradigm in healthcare, allowing telemonitoring systems the access, provision and management health information. Telemonitoring applications focused on the centralization of care in patients have advantages in accessing and providing healthcare. But conditions that safeguard security, privacy and confidentiality must be guaranteed so that patients, informal caregivers and healthcare professionals can trust the system.
To guarantee data security and privacy, it is necessary that the data model used by applications

for mobile health telemonitoring ensures that data is only accessed by those who need it and have the necessary access permission.

Acknowledgements

CITIC is funded by the Xunta de Galicia through the collaboration agreement between the Consellería de Cultura, Educación, Formación Profesional e Universidades and the Galician universities for the reinforcement of the research centres of the Galician University System (CIGUS).

Bibliography

H. Curado, P. Veloso Gomes, M. Jacquinet, A. Marques, and J. Pereira. Strategy for data cybersecurity in european health data ecosystem. In *Proceedings of V XoveTIC Conference. XoveTIC 2022*, volume 14 of *Kalpa Publications in Computing*, pages 35–37. EasyChair, 2023.

S. H. Houser, C. A. Flite, and S. L. Foster. Privacy and security risk factors related to telehealth services - a systematic review. *Perspectives in Health Information Management*, 1(20), 2023.

H. Lança. *Inteligência Artificial e Tecnologia no Mundo da Medicina: Prolegómenos*. Editora D'Ideias. ISBN: 978-989-53817-0-8, In Inteligência Artificial, Tecnologia e Cuidados de Saúde, coord. Inês Fernandes Godinho, António Tavares. - 1ª ed. - Coimbra. 93-104, 2022.

A. G. D. Pereira. *Consentimento informado e bens jurídicos no direito penal e no direito civil. In Consentimento informado em Direito Civil e Penal. Lopes, E.9-32*. Centro de Estudos Judiciários. ISBN: 978-989-9018-27-3. https://cej.justica.gov.pt/LinkClick.aspx?fileticket=kBS6KaykToo

J. Pool, S. Akhlaghpour, F. Fatehi, and L. C. Gray. Data privacy concerns and use of telehealth in the aged care context: An integrative review and research agenda. *International Journal of Medical Informatics*, 160, 2022.