

Recommendations for the protection of patient privacy

Gustavo Franco Carvalhal¹, Marcelino Hofmeister Poli², Fabiano Kingeski Clementel³, Gabriel Chittó Gauer⁴, Graziela Hax Marques⁵, Inês G. Silveira⁶, João Manuel Piccoli⁷, Lívia Haygert Pithan⁸, Luiz Gustavo Guilhermano⁹, Magda Ferreira¹⁰, Marcelo Bonhemberger¹¹, Maria Antonia Zancanaro de Figueiredo¹², Maria Estelita Gil¹³, Mariangela Badalotti¹⁴, Marcio Debiasi¹⁵, Paulo Vinícius Sporleder de Souza¹⁶, Raquel Milani El Kik¹⁷, Vera Maria Petersen¹⁸, Délio José Kipper¹⁹

Abstract

Concerns regarding the bioethical aspects of the privacy of the individual and the confidentiality of their medical treatment data is increasing in the medical community. The current preliminary clinical and therapeutic processes require the multidisciplinary involvement of a number of individuals, especially in the case of hospitalization. The transmission and storage of clinical and laboratory patient information involves different media, with inherent problems of accessibility and protection of information. The authors describe hypothetical situations that exemplify issues commonly addressed in the work of a clinical bioethics committee, contextualizing these problems in Brazil and globally, and suggest steps to minimize potential problems of the breaching of privacy and confidentiality.

Keywords: Bioethics. Medicine. Confidentiality. Privacy.

Resumo

Recomendações para a proteção da privacidade do paciente

A preocupação sobre aspectos bioéticos da privacidade do indivíduo e da privacidade dos dados de seus atendimentos é crescente no meio médico. Processos propedêuticos e terapêuticos atuais requerem envolvimento multidisciplinar de uma série de indivíduos, especialmente em se tratando de internações hospitalares. A transmissão e o armazenamento das informações clínicas e laboratoriais dos pacientes envolvem diferentes mídias, com problemas inerentes de acessibilidade e proteção da informação. Os autores sugerem situações hipotéticas que exemplificam problemas comumente abordados na atuação de comitê de bioética clínica, contextualizando-os no Brasil e no mundo, e sugerindo passos para minimizar potenciais problemas de quebra de privacidade e confidencialidade.

Palavras-chave: Bioética. Medicina. Confidencialidade. Privacidade.

Resumen

Recomendaciones para la protección de la privacidad del paciente

La preocupación sobre los aspectos bioéticos de la privacidad del individuo y de la confidencialidad de los datos de su asistencia está aumentando en la comunidad médica. Los actuales procesos clínicos y terapéuticos requieren la participación multidisciplinar de una serie de personas, especialmente en el caso de las internaciones hospitalarias. La transmisión y el almacenamiento de informaciones clínicas y de laboratorio de los pacientes implican diferentes canales de comunicación, con los problemas inherentes de accesibilidad y protección de la información. Los autores aluden a situaciones hipotéticas que ejemplifican problemas comúnmente tratados en el desempeño de un comité de bioética clínica, contextualizándolos en Brasil y en el mundo, y sugiriendo medidas para minimizar los posibles problemas de violación de la privacidad y de la confidencialidad.

Palabras clave: Bioética. Medicina. Confidencialidad. Privacidad.

1. **Doutor** gcarvalhal@terra.com.br – Pontifícia Universidade Católica do Rio Grande do Sul (PUCRS) 2. **Mestre** marcelino.poli@pucrs.br – PUCRS 3. **Doutorando** fabiano.clementel@pucrs.br – PUCRS 4. **Doutor** gabrieltgauer@gmail.com – PUCRS 5. **Mestre** graziela.hax@pucrs.br – PUCRS 6. **Doutora** ines.silveira@pucrs.br – PUCRS 7. **Mestre** joao.piccoli@pucrs.br – PUCRS 8. **Doutora** livia.pithan@pucrs.br – PUCRS 9. **Doutorando** luiz.guilhermano@pucrs.br – PUCRS 10. **Graduada** magssf@pucrs.br – PUCRS 11. **Doutorando** marcelo.bonhemberger@pucrs.br – PUCRS 12. **Doutora** antonia.figueiredo@pucrs.br – PUCRS 13. **Mestre** maria.gil@pucrs.br – PUCRS 14. **Doutora** mariangela.badalotti@pucrs.br – PUCRS 15. **Doutor** marciomed1@hotmail.com – PUCRS 16. **Doutor** pvsouza@pucrs.br – PUCRS 17. **Mestre** raquel.elkik@pucrs.br – PUCRS 18. **Graduada** veruskapetersen@hotmail.com – PUCRS 19. **Doutor** djkipper@pucrs.br – PUCRS, Porto Alegre/RS, Brasil.

Correspondência

Gustavo Franco Carvalhal – Rua Santo Inácio, 500/501 CEP 90570-150. Porto Alegre/RS, Brasil.

Declaram não haver conflito de interesse.

What represents privacy of patient data?

The right to the *privacy* of medical data guarantees the right of the individual to maintain information about themselves and their health problems inaccessible to other individuals¹. All information arising from medical interactions is considered confidential and access to it must be protected^{1,2}. Data on the health of the patient can only be consulted through their authorization or at the request of the legal system. When the patient cannot grant permission due to age or health questions, it can be provided by a legal representative or caregiver.

The protection of medical information in Brazil is based in law. In dealing with Fundamental Rights and Guarantees the Brazilian Constitution of 1988 ensures, in Chapter I, article 5, paragraph X, that *the privacy, private life, honor and image of persons are inviolable, and the right to compensation for material or moral damage resulting from their violation is assured*³. The confidentiality of medical data is also regulated in the “Charter of the Rights of Health Users” (“Carta dos Direitos dos Usuários da Saúde”) published by the Ministry of Health (Ministério da Saúde) and the National Health Council (Conselho Nacional de Saúde) in 2013. In article 4, item III, this document guarantees *a) physical integrity; B) privacy and comfort; C) individuality; d) ethical, cultural and religious values; E) the confidentiality of all and any personal information arising from medical consultations and diagnostic, preventive, surgical, therapeutic and hospitalization procedures*⁴.

Why is data privacy important?

The right to the privacy of medical information is increasingly relevant. According to Jane Kaye, *the protection of the privacy of the individual is highlighted in all the legal documents of liberal democracies and is a defining aspect of civil society*⁵. Violating the privacy of medical information can directly affect the life of any individual, with practical consequences. The disclosure of health data may, for example, influence the perception of others about the life expectancy of that person, about the possibility of developing certain diseases or disabilities, or about situations of paternity or maternity¹⁶. In addition, information about the existence of serious (e.g. chronic-degenerative,

infectious, neoplastic, or psychiatric) diseases, drug or drug use, or sexual options may generate discrimination, with possible deleterious effects on the patient both in the personal and social fields⁶.

With the accelerated development of molecular research, it is now possible to perform whole genome sequencing in a quick and relatively inexpensive manner. This sequencing can provide information on virtually all the protein variants encoded in the genome of the individual, in addition to those known to influence the emergence of various diseases or syndromes^{6,7}. Therefore, the protection of the privacy of individuals becomes even more important when we consider genetic research, as the data discovered there may affect not only the patient in question, but also their immediate family and future generations of that family^{6,8,9}.

The privacy of medical information is today so important that the obtaining of informed consent on the storage of clinical data is part of the process of practically every operation and clinical internment of a hospital institution. It is equally indispensable to any clinical or basic research protocol that includes the use of biological materials¹⁰⁻¹².

The use of medical information in basic, clinical or translational research has its own characteristics. There are documents regulating ethical principles in research that safeguard the protection of patient data^{11,12}. An example of this is the document published by the Council for International Organizations of Medical Sciences in 2002¹², which establishes that it is the duty of researchers to preserve the confidentiality of the data of patients involved in their research projects. This can be done in several ways: by omitting information that may lead to patient identification, limiting access to information or making it anonymous.

Patients have the right to expect researchers or health professionals to treat all information as confidential, providing it only when necessary to professionals involved in patient care who have the legal right to access such information. Some research, such as that carried out in seropositive patients in relation to the human immunodeficiency virus, can generate risks of social discrimination, which should be reduced as much as possible. The same can happen in research into cancer or genetic/hereditary conditions¹².

The problem of access to medical information

Traditionally, medical information was recorded in handwritten documents, called “medical records,” which were kept in the inpatient units and then stored in the medical record archive of the hospital. This posed some practical difficulties: the need for the physical presence of the medical records caused inconvenience, as they could only be accessed at any given time by a single professional or sector, and availability was not always easy or quick. This led to delays that were prejudicial to the clinical management of patients, obtaining data for research, and making records available for administrative and financial purposes^{1,13}.

With the computerization of medical records, access was improved, allowing simultaneous and rapid consultation by various sectors to the clinical, laboratorial, imaging and pathology data that was now integrated, reducing time and costs. There is also now the opportunity to minimize prescription and drug administration errors^{1,13}. However, security problems arising from the easier availability of data have been constant in hospitals, with unauthorized access, record corruption and misuse of medical information¹⁴. For illustration, let us imagine three hypothetical situations illustrating the recent difficulties in maintaining the privacy of data regarding hospital care.

• Situation 1

A patient is hospitalized in a hospital where they work. In three days, more than 400 accesses to the electronic medical record were identified, almost entirely by co-workers.

• Situation 2

A patient enters the psychiatric hospitalization unit of a university hospital for treatment. Family members contacted the medical team responsible to report that messages about the patient’s health status are being circulated in a WhatsApp group. The information was being passed to the group by a nursing assistant who knew the patient, who obtained the password to access the medical records through a nurse from the unit and transmitted daily messages.

• Situation 3

A student watches a birth performed at a university hospital and makes an amateur video recording of the event with a mobile phone,

posting a link to the video playback on his personal Facebook page.

Examining the three hypothetical situations in more detail, we can make several observations. In *situation 1*, there is a clear lack of confidentiality of medical information, which theoretically should be accessed only by professionals invited to provide care for the patient, with his or her knowledge and acquiescence. The possibility of access to the information contained in medical records by other professionals reveals glaring flaws in the medical information system in force in our hospitals. In *situation 2*, in addition to the access of medical information by an unauthorized caregiver, there is also unauthorized disclosure via social media. This latter occurrence is repeated in *situation 3*.

However, article 73 of the Code of Medical Ethics (Código de Ética Médica - CEM) published in 2009, prohibits the physician from *revealing the fact that he or she has knowledge in virtue of the exercise of his or her profession, except for just cause, legal duty or the written consent of the patient*¹⁵. Similarly, article 75 of the CEM states that it is forbidden for the physician to *refer to identifiable clinical cases, to exhibit patients or their profiles in professional advertising or through the dissemination of medical matters in forms of communication in a general sense, even with patient authorization*¹⁵. The proposed examples demonstrate the ease with which confidential and private information can be obtained and made public.

It is therefore clear that maintaining the security of medical information cataloged in electronic databases is a permanent challenge. To address the issue, access barriers with passwords and antivirus programs can be installed. The coding of data and the continuous monitoring of accesses to the computer system should also be encouraged. Furthermore, as shown by the examples given, the education of professionals involved in patient care is also critical. Access to medical records and electronic registers should be limited to what is needed to provide the best specific care, and the sharing of individual access passwords should be prohibited.

These measures limit the leaking of information and protect the privacy of the patient^{13,14}. In the three situations described, it can be presumed that article 78 of the CEM has not been respected at some point. This warns that doctors should not *fail to advise their assistants and students to respect professional secrecy and to ensure that they maintain it*¹⁵. The instantaneousness of the information propagated by social media allows the magnitude of these problems to quickly reach serious proportions and makes it

difficult to control problematic situations, as any corrective action is often delayed.

Overall, the current state of the protection of privacy of patient data is still precarious even in first world countries, where computerized medical data has been encouraged and implemented for several decades. In a systematic review carried out across several databases, Falcão-Reis, Costa-Pereira and Correia¹⁴ identified 49 English-language publications that discussed the safety and privacy of electronically stored medical data. They found that only 25 studies registered periodic audits of accesses in hospitals and clinics, and only four publications addressed the issue of educating physicians and other employees as a strategy for protecting privacy¹⁴.

Protection of patient privacy in Brazil

In Brazil, the issue of confidentiality of medical data and patient privacy has also received attention, despite a limited number of publications. Most of the texts state that confidentiality is the right of the patient and the duty of the physician¹⁵⁻¹⁸. It is a clear duty not only for professionals, but also for institutions. A US estimate has established that about 75 people utilize or come in contact with the data of a single patient during the hospital admission process¹⁹. The situation is no different in Brazilian hospitals. This is evidenced by the aforementioned Article 78 of the CEM¹⁵, which deals with the obligation to provide guidance for assistants and students about medical confidentiality, as well as article 107 of Resolution 1,246/1988²⁰.

The awareness of respect for patient confidentiality and privacy should be encouraged. In 2007, Loch, Clotet and Goldim¹⁶ published a cross-sectional survey of 711 university students from different undergraduate courses regarding confidentiality in adolescent care. While there were different responses about the importance of confidentiality in the care setting, 82% of respondents said they would only allow information to be transmitted to third parties with the consent of the patients.

In relation to unauthorized situations, they believed a breach of confidentiality would occur in cases of risk to the physical integrity of the patient or third parties, such as risk of suicide (85%), violence (84.2%), sexual abuse (81.7%), anorexia nervosa (81.3%) and threat to the life of others (72.3%). The numbers were lower in behavioral situations, such as drug use (51.7%), STD risk (44.7%) and homosexuality (20.7%),¹⁶.

Protecting patient privacy and medical information

While it is difficult to achieve perfect results in terms of the protection of the privacy and medical information of patients, suggestions made by several authors are outlined below. These suggestions were discussed by the members of the Clinical Bioethics Committee of the São Lucas Hospital of the Pontifical Catholic University of Rio Grande do Sul (Pontifícia Universidade Católica do Rio Grande do Sul - PUCRS):

- Educate professionals in the healthcare system;
- Secure access to patient information through individual authorization and passwords;
- Reinforce the concept that the access password is individual and should not be shared;
- Upon accessing the information, a message should warn the health professional about the possible legal consequences of the misuse of the same;
- Establish a surveillance system that can ensure that the user is accessing data pertinent to patients under their care;
- Disseminate concepts that value the privacy and confidentiality of medical data among future professionals in the field of health and information technology;
- Remember that it is up to the patient to decide which of his/her data may be made available, to whom and under what circumstances.

Final considerations

In a world in which medical knowledge is constantly increasing, where information is transmitted almost instantaneously via a variety of media, and where the judicialization of healthcare is increasingly prevalent, concern for bioethical aspects is becoming increasingly relevant. Protecting the privacy of medical information requires ongoing attention and education from healthcare professionals and those involved in the acquisition, use, and storage of patient health data. As patients are the principal parties of interest in their own health, they have the right to decide on the content, the recipient and the circumstances of the availability of their data.

Referências

1. Ozair FF, Jamshed N, Sharma A, Aggarwal P. Ethical issues in electronic health records: a general overview. *Perspect Clin Res.* 2015;6(2):73-6.
2. Buckovich SA, Rippen HE, Rozen MJ. Driving toward guiding principles: a goal for privacy, confidentiality, and security of health information. *J Am Med Inform Assoc.* 1999;6(2):122-33.
3. Brasil. Presidência da República. Constituição da República Federativa do Brasil, de 5 de outubro de 1988. [Internet]. Diário Oficial da União. Brasília, 5 out 1988 [acesso 2 dez 2015]. Disponível: <http://bit.ly/1dFiRrW>
4. Brasil. Ministério da Saúde. Conselho Nacional de Saúde. Carta dos direitos dos usuários da saúde. [Internet]. 4ª ed. Brasília: Ministério da Saúde; 2013 [acesso 2 dez 2015]. Disponível: <http://bit.ly/1jfWeyl>
5. Kaye J. The tension between data sharing and the protection of privacy in genomics research. *Ann Rev Genomics Hum Genet.* 2012;13:415-31. p. 416. PMID: 22404490.
6. Kaye J. Op. cit.
7. Cambon-Thomsen A. The social and ethical issues of post-genomic human biobanks. *Nat Rev Genet.* 2004;5:866-73.
8. Arnason V. Coding and consent: moral challenges of the database project in Iceland. *Bioethics.* 2004;18(1):27-49.
9. McGuire AL, Fisher R, Cusenza P, Hudson K, Rothstein MA, McGraw D *et al.* Confidentiality, privacy, and security of genetic and genomic test information in electronic health records: points to consider. *Genet Med.* 2008;10(7):495-9.
10. Beskow LM, Burke W, Merz JF, Barr PA, Terry S, Penchaszadeh VB *et al.* Informed consent for population-based research involving genetics. *Jama.* 2001;286(18):2315-21.
11. International Committee of Medical Journal Editors. Recommendations: Protection of research participants. [Internet]. 2015 [acesso 4 dez 2015]. Disponível: <http://bit.ly/1rBoe0S>
12. Council for International Organizations of Medical Sciences. International ethical guidelines for biomedical research involving human subjects. [Internet]. Geneva: Cioms; 2002 [acesso 7 jan 2016]. Disponível: <http://bit.ly/2l6h1bj>
13. Fernández-Alemán JL, Señor IC, Lozoya PÁ, Toval A. Security and privacy in electronic health records: a systematic literature review. *J Biomed Inform.* 2013;46(3):541-62.
14. Falcão-Reis F, Costa-Pereira A, Correia ME. Access and privacy rights using web security standards to increase patient empowerment. *Stud Health Technol Inform.* 2008;137:275-85.
15. Conselho Federal de Medicina. Resolução nº 1.931, de 17 de setembro de 2009. Aprova o código de ética médica. [Internet]. Diário Oficial da União. Brasília, 24 set 2009 [acesso 7 jan 2016]. Disponível: <http://bit.ly/1ljjin7>
16. Loch JA, Clotet J, Goldim JR. Privacidade e confidencialidade na assistência à saúde do adolescente: percepções e comportamentos de um grupo de 711 universitários. *Rev Assoc Med Bras.* 2007;53(3):240-6.
17. Loch JA. Confidencialidade: natureza, características e limitações no contexto da relação clínica. *Bioética.* 2003;11(1):51-64.
18. Francisconi CF, Goldim JR. Aspectos bioéticos da confidencialidade e privacidade. In: Costa SIF, Oselka G, Garrafa V, coordenadores. *Iniciação à bioética.* Brasília: CFM; 1998. p. 269-84.
19. O'Rourke KD. *A primer for health care ethics: essays for a pluralistic society.* Washington: Georgetown University Press; 1995.
20. Conselho Federal de Medicina. Resolução nº 1.246, de 8 de janeiro de 1988. Aprova o código de ética médica. Diário Oficial da União. Brasília, p. 1574-7, 26 jan 1988. Seção 1.

Participação dos autores

Todos os autores participaram ativamente da discussão do tema, elaboração e revisão do manuscrito.

