International Journal of Nursing Sciences 7 (2020) 112–115

HOSTED BY

Contents lists available at ScienceDirect

International Journal of Nursing Sciences

journal homepage: http://www.elsevier.com/journals/international-journal-of-nursing-sciences/2352-0132

Discussion

Psychiatric electronic health records privacy in Jordan: A policy brief

Ahmed R. Karajeh [*], Majd T. Mrayyan

Department of Community and Mental Health Nursing, The Hashemite University, Jordan

ARTICLE INFO

Article history:
Received 8 February 2019
Received in revised form
27 November 2019
Accepted 7 December 2019
Available online 10 December 2019

Keywords:
Access to information
Electronic health records
Health informatics
Jordan
Privacy

ABSTRACT

Psychiatric health records are highly sensitive data which requires special policy to maintain its privacy, without affecting data accessibility. The current authors reviewed social, ethical and legal underpinnings for psychiatric electronic health records (EHR), and suggests a policy to maintain privacy and confidentiality of the psychiatric data, without affecting data accessibility. The purpose of this policy brief is to discuss and provide alternatives regarding psychiatric electronic health records privacy and information access. The current policy applied in Jordan still immature to ensure high levels of reliability, as the psychiatric data is openly accessed to the non-specialized personnel. Sensitive personal data policy is recommended in this paper with developing overriding mechanisms to counteract obstacles to data accessibility.

What is known?

- The current policy applied in Jordan still immature to maintain high levels of reliability without any special policy to maintain privacy of the psychiatric electronic health records.
- The current policy applied in the Ministry of Health of Jordan to keep privacy of electronic health records used passwords and access codes.
- The national program of electronic health records “HAKEEM” classifies the patients’ profiles to non-sensitive and sensitive patients. Information can be accessed under tracking and the patient can lock their data upon request. Thus, either the electronic health records is totally restricted or it is openly accessed even for non-specialized persons.

What is new?

- The current manuscript suggests the policy of sensitive personal data policy as a new policy in order to maintain high levels of privacy for psychiatric electronic health records. This policy will categorize the medical records (not the patients) as personal data and sensitive data, which consists of racial and ethnic origin, mental health, addiction, illness history, and sexual life; these data follow a preliminary declaration and authorization regime for the processing of sensitive health data.
- The current manuscript provides recommendations for the government, stakeholders, social media and health care providers in order to enhance work flow and social trust to the electronic form of the health data.

1. Executive summary

Policy is defined as a group of guidelines set by authorities in order to direct human behaviors toward particular goals, while a policy brief is a short document written for non-specialists to outline the rationale for choosing a particular policy alternative in a current policy debate [1]. According to Richard Rognehaugh, privacy is “The right of individuals to keep information about themselves from being disclosed to others; the claim of individuals to be let alone, from surveillance or interference from other individuals, organizations or the government.” [2] Psychiatric illness is a health condition that is associated with changes in emotions, thinking, and behaviors, and may involve distress and social and work dysfunction [3]. Electronic Health Records (EHRs) are a systematic electronic collection of clients’ health information in a digital format [4].

EHRs create an assurance for health care delivery systems: that they will provide more effective access to patients’ information, and they will improve data safety and work efficiency, as well as

[*] Corresponding author.
E-mail addresses: ahmed.karajeh@gmail.com (A.R. Karajeh), mmrayyan@hu.edu.jo (M.T. Mrayyan).
Peer review under responsibility of Chinese Nursing Association.

https://doi.org/10.1016/j.ijnss.2019.12.002
2352-0132/© 2020 Chinese Nursing Association. Production and hosting by Elsevier B.V. All rights reserved.

health quality [4]. However, despite all the benefits, psychiatric electronic data is still a point of contention because of the trade-off between the flexibility of EHRs and privacy issues, especially if we consider that data are constantly connected and saved in complex systems which increase vulnerability and risk of breakthrough, even from systems administrators themselves.

Migration from paper-based records to electronic forms of databases results in privacy and informational access issues, especially for psychiatric patients [5]. Despite using several approaches to maintain the privacy and safe use of EHRs, there is still not an obvious special policy aimed to guarantee psychiatric electronic health record privacy. In addition, health care employees have access to all health data—even psychiatric data—because those systems are often designed for non-psychiatric patients.

The purpose of this policy brief is to discuss and provide alternatives regarding psychiatric patient electronic health record privacy and informational access.

2. Context and importance of the problem

Issues of privacy and confidentiality have become more significant after recent technological advancements, including medical data-sharing and the compilation of electronic health records. In the reports of the U.S. Department of Health & Human Services Office of Civil Rights (OCR) it was clearly stated that using EHRs should not conflict with maintaining the privacy and security of health information [6]. Locally, Electronic Health Solutions (EHS) is a not-for-profit organization implementing a national wide EHR system called Hakeem®; this is considered the only organization which provides full EHR services in Jordan [7]. Lama Al-karmi, a quality manager at EHS, in a personal interview (15 Jan 2019) stated that the usage of EHRs could actually enhance the security of patients' health care information compared with paper-based files which can be accessed randomly at patient wards or other locations; however, a complex online security breach could happen to electronic medical records.

Since the time of Sigmund Freud, psychiatric care providers have struggled with how written information and documentation of psychotherapy findings affect patients' openness in sessions, and how much information should be documented; concerns about privacy and confidentiality have been a great barrier in to adoption of EHR for mental health illnesses [8,9].

Salmon and colleagues, in their study about psychiatrists' views about EHR adoption, said that the majority of psychiatrists expressed privacy concerns after the adoption of EHR; 63% of psychiatrists express low willingness to record confidential information in an EHR, and 83% of psychiatrists require modifications and limited access to their patients' sensitive data [8]. In fact, stigma is one of several reasons why psychiatric patient treatment is fragmented from other medical illnesses. Stigma affects treatment plans and the patient care landscape. Thus, stigma has been a great barrier for utilizing EHR in psychiatric care facilities; even psychiatrists resist integrating sensitive data in EHRs [10].

Therefore, in the literature, ethical and legal obligations are still a concern with regard to patients' confidential information being illegally accessed by unauthorized personnel. Milton discussed the need to set clear guidelines, policies, and procedures to regulate access to patient information, including care recipients' rights to access their own records [11].

2.1. Social context

Access to patients' information is a public issue because it may impact anybody seeking health care services. In 2019, a recent study published in the *Journal of Medical Ethics* revealed that sensitive data exposure online often results in anxiety, depression, and PTSD [12]. Unauthorized access to and the resulting disclosure of health-care–related information have great social effects on individuals and groups, especially given the stigma associated with mental health diseases [13].

Breaches of cloud storage of health records cannot be underestimated. Serious consequences have been seen after pure dissemination of sensitive data; a medical advisor in SMM Health Ltd. reported that numerous patients developed mental issues after privacy breaches via unauthorized use of cloud storage and others required medical treatment. Furthermore, a significant psychological impact has been noted in patients whose sensitive data are not treated correctly—the damage surpasses financial loss and psychosocial harm [14].

2.2. Ethical context

EHRs may provide beneficence, but conflicts with ethical principles exist. Autonomy is breached when personal information is accessed without patient consent for any reason. Fidelity is jeopardized through exposure of thousands of records due to breakthroughs or unauthorized access. According to the utilitarian point of view justification, patients reveal their personal information to their physicians seeking diagnoses and treatment; they trust that their data will not be disclosed to other parties [15]. In the absence of a privacy guarantee, patients would hide important information in diagnosis and treatment, or even stop coming to the health care meetings. Considering this in relation to psychiatric electronic health records, the patient–physician relationship is one of the most important and essential pillars of health care which should be facilitated and supported by EHRs [16]. Patients with paranoia or psychosis consider the feeling of surveillance to be a trigger and can cause an acute psychotic episode. For instance, for patients with chasing delusion, maintaining their trust is very important and hard to achieve if those patients know that their information is stored on the cloud and others can skim or breach it; this would surely result in a loss of trust in the health care facility overall and cause them to hide bizarre behaviors, feelings, plans, and other important information from the psychiatrist, which may adversely affect correspondence, transparency, and treatment plan commitment [14,17].

2.3. Political and legal context

The U.S. Federal Government put in place the Health Insurance Portability and Accountability Act of 1996(HIPAA) to ensure that patients have rights over their health information regardless of the form of information(i.e., whether electronic or paper-based). The security rule of HIPPA requires specific protection procedures to safeguard electronic health information (i.e., passwords and PIN codes). Moreover, U.S. federal law requires doctors, hospitals, and other health care providers to notify the patient in cases of unauthorized breaches or access to their health-related information. The law also requires the health care provider to notify the authorities and the media if a breach affects more than 500 residents of a state or jurisdiction. These requirements help patients know if something has gone wrong with the protection of their information and helps keep providers accountable for EHR protection [7].

Many efforts addressed to counteract privacy issue in psychiatric electronic health records. The federal standards clarify a clear boundary between psychotherapy notes and medical notes; as a part of that, in April 2003, HIPPA rule 45 CFR 164.501 [18] was introduced and the new standards put in place obvious boundaries between medical notes and psychotherapy notes, and determined that psychotherapy notes should not be kept with regular medical notes and must not be released without the written authorization of the patient. This authorization was inspired by the landmark 1966 court case, *Jaffeev. Redmond*; the court suppressed a request from the victim's family in order to access psychiatric records of a police officer who had shot a man after being involved in an altercation [19]. Furthermore, the U.S. Department of Mental Health and Human Services(HHS) published, in July 26, 2013, an "interim final" rule that regulates when and how psychologists and other parties covered by HIPPA must notify patients and the HHS when protected psychiatric information is exposed by an unauthorized breach in a way which results in significant risk of patient harm [20].

In Jordan, the Ministry of Health issued a policy in July 2013 that regulates EHRs, protection of patient information, and e-prescriptions. The policy ensures that the sites where EHRs are implemented should use the primary patient file (replacing the paper-based version) to set up the protection procedure of access codes and assure the accountability and liability rules of the access given to any health care worker.

3. Policy implications and relevance

Currently, psychiatric patients are considered the most stigmatized patients because of the public view of their illnesses; this brings up the debate between the need for EHRs and poor protection of sensitive data. Therefore, Jordanian psychiatric patients need a special policy to maintain privacy and protection of their electronic health records. In an interview with the author (15 Jan 2019), Mamdouh Al-saideh, an information security manager at Hakeem—the only completely Jordanian model of an EHR system—said that Hakeem maintains patients' information privacy through classifying the patients as non-sensitive and sensitive patients; information can be accessed under tracking and the patient can lock their data upon request. Hence, the psychiatric data is openly accessed in most cases, even for non-psychiatrists, which puts privacy at risk from snooping. Consequently, a sensitive personal data policy requires a great amount of attention in this case.

4. Critique of policy options

There are various law requirements about how medical information should be kept and at what level of security it needs to be stored. Some data are kept as open-access data and other data need to be secured. Here, a conflict between data security versus data accessibility has emerged. Thus, it is important to know which data are sensitive and which data can be openly accessed. Great care regarding a sensitive personal data policy is needed in this context.

A sensitive personal data policy will categorize the medical records(not the patients) as personal data and sensitive data which consist of racial and ethnic origin, mental health, addiction, illness history, and sexual life; these data follow a preliminary declaration and authorization regime for the processing of sensitive health data. The main problem in the current model is that it could impede the workflow of health careproviders, especially in emergency situations. Other negative consequences include hiding patients' destructive behaviors could put other staff at risk of violence, some psychiatric patients cannot provide consent because of their illnesses, and there will be extra workload for the system database.

5. Policy recommendations

The following recommendations are presented in order to improve and regulate the use of sensitive personal data to accommodate psychiatric illnesses.

To begin with, processing data should be prohibited by default, unless exceptions apply, such as "explicit consent." Where explicit consent is needed from the attending psychiatrist, who owes the duty of confidentiality to use pre-encrypted psychiatric data. Should carry out encryption without using the patient's real name. Explicit consent should be limited to sensitive personal data, but other personal data is reclaimed under the applied privacy policy. In addition, system administrators should track any access to patients' sensitive data and have a responsibility to report any data breach; this breach should be subject to a strict law with legal sanctions. This policy should be circulated among all health care facilities by the government. As evidenced, the American Health Information Management Association in their 2008 functional toolkit reported that the audit trait should be carried out across all system activities; these activities should be tracked by audit trails on a random and regular basis and be compliant with hospital policy [21]. Moreover, U.S. HHS rule 46 CFR section 164.308 stresses that when there is an unauthorized access of medical records the system will track this access by recording the name of the person, time, date, screens accessed, and duration of access; if this is proven to be illegitimate access there will be legal consequences [22].

Secondly, warning signs appear on patient files in order to notify any other staff if they have any violent behaviors toward themselves or others, or a life-threatening condition. Further, the media must educate the public about how their sensitive data is kept according to the new policy, in order to improve public opinion about the high security of electronic databases.

Finally, a sensitive personal data policy would help to maintain high levels of privacy for psychiatric patients' electronic information. The researchers advise policymakers to take the listed recommendations into consideration in order to avert problems with work flow.

CRediT authorship contribution statement

Ahmed R. Karajeh: Conceptualization, Writing - original draft, Writing - review & editing. **Majd T. Mrayyan:** Conceptualization, Writing - original draft, Writing - review & editing, Supervision.

Acknowledgements

The current author just would like to express his thanks and gratitude to the Hashemite University and to the most influential professors for their encouragement and support throughout completing his master study.

Appendix A. Supplementary data

Supplementary data to this article can be found online at https://doi.org/10.1016/j.ijnss.2019.12.002.

References

[1] Mason DJ, Leavitt J, Chaffee M. Policy & politics in nursing and health care. fifth ed. Elsevier Health Sciences; 2007.

[2] Rognehaugh Richard. The health information technology dictionary. Wolters Kluwer Law & Business; 1999. p. 175.

[3] American Psychiatric Association. DSM-5®). In: Diagnostic and statistical manual OF mental disorders. Washington, DC: American Psychiatric Publishing; 2013. p. 947.

[4] Institute of Medicine (US) Committee on Data Standards for Patient Safety. Key capabilities of an electronic health record. Key capabilities of an electronic health record system: letter report. 2003. Washington (DC).

[5] Jha AK, DesRoches CM, Campbell EG, Donelan K, Rao SR, Ferris TG, et al. Use of electronic health records in U.S. Hospitals [Internet] N Engl J Med 2009 Apr 16;360(16):1628–38. Available from: http://www.nejm.org/doi/abs/10.1056/NEJMsa0900592.

[6] U.S. Department of Health & Human Services Office for Civil Rights. OFFICE rights for civil privacy, security, and electronic health records 1 privacy, security, and electronic health records. 2015.

[7] Hakeem program. Electronic health Solutions. Technology for better healthcare in Jordan [Internet]. 2015 [cited 2016 Apr 4]. Available from: www.ehs.com.jo/en/content/hakeem-1.

[8] Salomon RM, JU Blackford, Rosenbloom ST, Seidel S, Clayton EW, Dilts DM, et al. Openness of patients' reporting with use of electronic records: psychiatric clinicians' views [Internet] J Am Med Inform Assoc 2010 Jan 1;17(1):54–60. Available from: https://academic.oup.com/jamia/article-lookup/doi/10.1197/jamia.M3341.

[9] Freud S, Corporation SL. In: Strachey J, Freud A, Rothgeb CL, editors. The standard edition of the complete psychological works of Sigmund Freud, 21. Michigan: Hogarth Press; 1961. p. 287.

[10] Buntin MB, Burke MF, Hoaglin MC, Blumenthal D. The benefits of health information technology: a review of the recent literature shows predominantly positive results [Internet] Health Aff 2011 Mar;30(3):464–71. Available from: http://www.healthaffairs.org/doi/10.1377/hlthaff.2011.0178.

[11] Milton CL. Information sharing [Internet] Nurs Sci Q 2009 Jul 30;22(3):214–9. Available from: http://journals.sagepub.com/doi/10.1177/0894318409337026.

[12] Aboujaoude E. Protecting privacy to protect mental health: the new ethical imperative [Internet] J Med Ethics 2019 Sep 1;45(9):604–7. Available from: http://jme.bmj.com/content/45/9/604.abstract.

[13] Dalky HF. Arabic translation and cultural adaptation of the stigma-devaluation scale in Jordan. J Ment Health 2012;21(1):72–82.

[14] Walsh R. Data privacy: is it a mental health issue? [Internet]. 2019 [cited 2019 Sep 5]. Available from: proprivacy.com/privacy-news/data-privacy-mental-health-concern.

[15] Gillon R. Philosophical medical ethics [Internet] BMJ 1985 Jun 22;290(6485). 1904–1904. Available from: http://www.bmj.com/cgi/doi/10.1136/bmj.290.6485.1904-d.

[16] Sulmasy LS, López AM, Horwitch CA. Ethical implications of the electronic health record: in the service of the patient [Internet] J Gen Intern Med 2017 Aug 20;32(8):935–9. Available from: http://link.springer.com/10.1007/s11606-017-4030-1.

[17] Appelbaum PS. Privacy in psychiatric treatment: threats and responses [Internet] Am J Psychiatry 2002 Nov;159(11):1809–18. Available from: http://psychiatryonline.org/doi/abs/10.1176/appi.ajp.159.11.1809.

[18] U.S. Department of Health & Human Services Office for Civil Rights. 45 CFR subpart E - privacy of individually identifiable health information, vol. 164; 2000. p. 522.

[19] Chan K. Jaffee v. Redmond: making the courts a tool of injustice? J Am Acad Psychiatry Law 1997;25(3):383–9.

[20] U.S. Department of Health & Human Services Office for Civil Rights. Breach notification rule [Internet], 2013 [cited 2019 Oct 1]. Available from: https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html.

[21] American Health Information Management Association. Copy functionality toolkit. 2008. 2008.

[22] U.S. Department of Health & Human Services Office for Civil Rights. Security standards: general rules. 46 CFR section 164.308(a)-(c) United States.