Medical Informatics 2018 - INFORMATION SECURITY AND PATIENT PRIVACY: CRUCIAL ISSUE IN HEALTHCARE MANAGEMENT

Pinar Kilic Aksu - Yeditepe University, Turkey, Email Id: pinarkilicaksu@yahoo.com

Abstract

Technologies for information security are actively used in organizations where information is intensely used. Information security covers the entire process of protection, processing, and transmission of information within organizations. The information security process starts with a security policy designed to protect the organization's general assets. Information security policies include rules and practices on obligations of employees, the use of security control instruments and the management of process. In healthcare management, information management systems provide the information needed at each stage of processes related to health care activities. Hospital Information Management Systems (HIMS) are an example for the use of information and communication technology in healthcare. Hospitals are complex structures where multiple functions are carried out together. As well as keeping a complete medical record, basic functions of hospital information management system can be listed as keeping financial records, using resources properly, increasing the service quality, provision of information support for important decisions for clinicians and managers. In this frame, information security and patient privacy are critical points for these functions in healthcare management.

This work is presented at 3rd International Conference on e-Health and Alternative Healthcare Innovations (E-HEALTH – 2020 Webinar) on October 12-13, 2020

The Value and Importance of Health Information Privacy

Ethical health research and privacy protections both provide valuable benefits to society. Health research is vital to improving human health and health care. Protecting patients involved in research from harm and preserving their rights is essential to ethical research. The primary justification for protecting personal privacy is to protect the interests of individuals. In contrast, the primary justification for collecting personally identifiable health information for health research is to benefit society. But it is important to stress that privacy also has value at the societal level, because it permits complex activities, including research and public health activities to be carried out in ways that protect individuals' dignity. At the same time, health research can benefit individuals, for example, when it facilitates access to new therapies, improved diagnostics, and more effective ways to prevent illness and deliver care.

The intent of this chapter[1] is to define privacy and to delineate its importance to individuals and society as a whole.

Patient Attitudes About Privacy in Health Research

In summary, very limited data are available to assess the privacy value of the Privacy Rule provisions that impact researchers. Surveys indicate that the public is deeply concerned about the privacy and security of personal health information, and that the HIPAA Privacy Rule has perhaps reduced—but not eliminated—those concerns. Patients were generally very supportive of research, provided safeguards were established to protect the privacy and security of their medical information, although some surveys indicate that a significant portion of the public would still prefer to control access to their medical records via consent, even if the information is anonymized. Studies indicate that public support for research and willingness to share health information varies with health status and the type of research conducted and depends on the patients' trust

that their information will be kept private and confidential.

CONCLUSIONS AND RECOMMENDATIONS

Based on its assessment of the records described on this chapter, the committee agreed on an overarching principle to guide the formation of recommendations. The committee affirms the importance of preserving and improving the privateness of fitness statistics. In the context of fitness research, privacy consists of the commitment to address personal records of sufferers and studies contributors with meaningful privacy protections, including strong protection measures, transparency, and duty.16 These commitments enlarge to everyone who collects, uses, or has get admission to to in my opinion identifiable health records of patients and research participants. Practices of security, transparency, and accountability take on awesome importance in the fitness research setting: Researchers and other statistics users should disclose virtually how and why personal data is being collected, used, and secured, and have to be difficulty to legally enforceable obligations to ensure that individually identifiable facts is used accurately and securely. In this manner, privateness safety will help to make certain studies participation & public accept as true with and self-assurance in medical studies.

As a part of the procedure of enforcing this principle into the federal oversight regime of health studies, the committee recommends that each one establishments inside the fitness research network which are concerned inside the collection, use, and disclosure of for my part identifiable fitness facts need to take strong measures to safeguard the security of fitness data. For example, establishments could:

• Appoint a protection officer responsible for assessing information protection desires and enforcing answers and workforce training.

• Make more use of encryption and different strategies for records security.

• Include records safety specialists on IRBs.

• Implement a breach notification requirement, so that sufferers can also take steps to guard their identity inside the event of a breach.

• Implement layers of security protection to take away single factors of vulnerability to safety breaches.

• Genuine privacy-enhancing strategies that minimize or put off the gathering of individually identifiable statistics.

• Standardized self-evaluations and security audits and certification applications to assist institutions acquire the goal of safeguarding the safety of private health information.

Effective fitness privacy protections require effective records security measures. The HIPAA Security Rule (which entails a set of regulatory provisions separate from the Privacy Rule) already units a ground for facts security standards within protected entities, but no longer all establishments that behavior fitness research are concern to HIPAA regulations. Also, the survey information presented on this chapter show that neither the HIPAA Privacy Rule nor the HIPAA Security Rule have directly improved public confidence that personal health facts might be saved confidential. Therefore, all institutions conducting fitness research must undertake measures to strengthen records protections. For example, given the latest spate of lost or stolen laptops containing patient health facts, encryption must be required for all laptops and detachable media containing such data. However, in general, given the differences a few the missions and sports of establishments within the health research network, some flexibility in the implementation of unique safety measures will be necessary.

REFERENCES

1. Aggarwal CC, Yu PS, editors. Privacy-preserving records mining: Models and algorithms. Boston, MA: Kluwer Academic Publishers; 2008.

2. AHIMA (American Health Information Management Association). The country of HIPAA privateness and security compliance.

3. Allen A. Genetic privacy: Emerging ideas and values. In: Rothstein M, editor. Genetic secrets: Protecting privateness and confidentiality in the genetic era. New Haven, CT: Yale University Press; 1997. Pp. 31–59.

4. Balch GI, Doner L, Hoffman MK, Macario E. An exploration of ways sufferers and family caregivers consider counterfeit drugs and the safety of prescription drug stores for the National Health Council. Oak Park, IL: Balch Associates; 2005.

5. Balch GI, Doner LMA, Hoffman MK, Merriman MP, Monroe-Cook E, Rathjen G. Concept and message development studies on engaging groups to promote electronic non-public health information for the National Health Council. Oak Park, IL: Balch Associates; 2006.

6. Bodger JA. Note, taking the sting out of reporting requirements: Reproductive fitness clinics and the constitutional proper to informational privacy. Duke Law Journal. 2006;56:583–609. [PubMed]

7. Burkert H. Privacy-enhancing technologies: Typology, critique, vision. In: Agre PE, Rotenberg M, editors. Technology and privacy: The new landscape. Cambridge, MA: The MIT Press; 2001. Pp. 125–142.

8. Claerhout B, De Moor GJE. Privacy protection for medical and genomic statistics: The use of privateness-enhancing techniques in medicine. Journal of Medical Informatics. 2005;74:257–265. [PubMed]

9. Conn J. CMS' HIPAA watchdog presents ability conflict. Modern Healthcare. 2008. [accessed July 28, 2008]. Http://www.Modernhealthcare.Com .

10. Melek A, MacKinnon M. Deloitte global protection survey. 2006. [accessed July 23, 2008]. Http://www.Deloitte.Com/dtt/cda/doc/content/us_fsi_150606globalsecuritysurvey(1).Pdf .

11. Metz R. Google makes fitness carrier publicly available. Associated Press; 2008. [accessed August 13, 2008]. Http://biz.Yahoo.Com/ap/080519/google_health.Html .

12. Nissenbaum H. Privacy as Contextual Integrity. Washington Law Review. 2004;79:101–139.

13. NRC (National Research Council). Improving get admission to to and confidentiality of studies data: Report of a workshop.

14. NRC. Who is going there?: Authentication through the lens of privateness..

15. NRC. Expanding get admission to to studies facts: Reconciling dangers and opportunities.

16. NRC. Engaging privateness and statistics era in a digital age. . NRC. Privacy and records technology in a digital age.

17. NRC. Putting humans at the map: Protecting confidentiality with related social-spatial facts.

18. OCR (Office for Civil Rights). HIPAA compliance and enforcement. 2008. [accessed August 13, 2008]. Http://www.Hhs.Gov/ocr/privacy/enforcement/

19. OIG (Office of Inspector General). Nationwide overview of the Centers for Medicare & Medicaid Services Health Insurance Portability and Accountability Act of 1996 oversight. Washington, DC: Department of Health and Human Services; 2008.

20. OTA (Office of Technology Assessment). Protecting privateness in automatic medical records. Washington, DC: OTA; 1993.

21. Petrila J. Medical records confidentiality: Issues affecting the mental fitness and substance abuse systems. Drug Benefit Trends. 1999;11:6–10.

22. Post R. Three concepts of privacy. Georgetown Law Journal. 2001;89:2087–2089.