Hipaa: as it relates to it research paper examples

Law, Security

Abstract

The following article is a brief discussion over the subject of Health Insurance Portability and Accountability Act Of 1996, (HIPAA, 1996) as it describes the use of Information Technology (IT) in the field of Healthy Care and dictates the security issues that IT must keep in mind for the general public health. Also discussed in the article are the importance of the IT industry in the present scenario practical implications and hurdles that IT must face in applying HIPAA health privacy guidelines, as well as, its impact upon the masses as a whole.

HIPAA

As it relates to IT

HIPAA (1996) act gives the right to have medical privacy to individuals from age 12 onwards. According to this Act, the one who provides health related information of an individual, must have a verified disclosure in the form of signatures from the individual has been affected, before the provider lends out any of the recorded information on health care facilities availed to the individual, including the individual’s family members. HIPAA aims to make changes to the Internal Revenue Code of 1986 so that it could improve shifting and continuity of health insurance services in both group and individuals, to combat wastage, fraudulence, and misuse of privileges in health insurance and health care service, to encourage the use of medical savings accounts, to improve access to long-term care services and coverage, to simplify the administration of health insurance, and for other purposes.

The ever increasing use of IT is rapidly spreading through societies; penetrating noticeably in educational institutes, government establishments, business group, homes and offices and health care industries. The implication of these developments is obvious in the sense that traditional ways of doing things, which have been embraced in the past, must now give way and/or adjust to the diverse opportunities offered by IT. The impact of IT on individuals, group and society has changed everything drastically and hence has led to the fact that IT must be regulated. HIPAA (1996) imposes regulations on to the use of Public Health, known as Health Information Technology, which is a service created to provide medical information of individuals to health services for various applications, which may include health policies, medical treatment etc.

Discussion

SEC. 1171. of Part C of the HIPAA defines and recognizes health information as

The term 'health information' signifies any information, by word of mouth or recorded over any type or medium, that-"

- Has been created or accepted by a health care provider, health policies, public health authorities, employment provider, life insuring firm, school or university, or health care clearinghouse; and

- Relating to the past, present, or future physical or mental health condition or conditions of an individual, provisional health care to an individual, or the previous, present, or intended payment for the facility of health care towards the demanding individual (HIPAA, 1996).

In a 1999 survey of consumer attitudes toward health privacy, 75%

respondents reported that they had significant worries about the privacy and concealment of their medical records (Forrester Research, 1999). In a survey comparatively more recent, which was conducted in 2005 after the implementation of the HIPAA Privacy Rule, a little more than 65 percent of the survey respondents said they still had concerns about the privacy of their medical records, directly putting in a suggestion that the Privacy Rule may not have effectively alleviated public concern about health information and privacy. Minorities, both ethnic and racial, showed the greatest concern among the respondents. Moreover, the survey revealed the fact that a large number of consumers were unfamiliar with the HIPAA privacy scheme coverage. Approximately 60 percent of participants reminisced receiving a HIPAA privacy notice, and only 27 percent believed they were entitled to lesser rights than they had before they received the privacy policy notice.

The HIPAA Security Rules and Boundaries

The goals of security are to ensure firstly that only individuals with legal authority see stored data, secondly the data should be visible only for a legally valid purpose, and thirdly but most importantly, accuracy. In practice, this criterion has been followed through protections with intentions of making data processing safe from unauthorized accessing, changing, omitting, or transmitting. The HIPAA Security Rule applies this traditional approach to protect security, and sets a strong niche for information security standards within applicable bodies. (Nass and Gostin, 2009)

It is clear from the facts above stated that though the general public either aware incompletely or unaware of the Privacy Protection that HIPAA provides them with, they are aware of the fact that personal information and its safety is a major concern and priority. Individuals are concerned about the safety of the personal information that their medical records may contain, and the misuse that may be done with such valuable information, as information in the current age of IT is an asset similar to gold. With more and more sophisticated data acquisition and higher data transfer throughout networks, any form of information becomes highly valuable to who so ever gets a hold of it. Therefore security is an issue that must be addressed particularly in the case of Health Data. (Nass and Gostin, 2009)

HIPAA Scope Checklist (Federal Register, 2001)

The HIPAA Security Rule stipulates a list of compulsory or addressable safety measure.

Following is checklist of some of the provisions that a Health Service Information group must comply with:

- Are the groups considered as a covered body under HIPAA (Health Insurance Portability and Accountability Act)?
- Do the groups have a designated spokesperson or office that is responsible for receiving grievances?
- Are grievances acknowledged?
- Is the nature of grievances documented?
- Do the groups have policies and measures according to secured health information that are designed to comply with HIPAA standards and application conditions?
- Do the groups alleviate, to the practical extent, any damaging effect that a use or release of protected health information is in defilement of its policies and processes?

- Do the groups have a six-year retaining period for HIPAA-related records?

- Are the groups providing the suitable training to its employees on policies and procedures with respect to protected health information?

- Are notices made available on the uses and disclosures of protected health information?

- Do the notices cover:

- Descriptions of uses, disclosures, and purposes?

- Statements of the individual’s rights?

- Statements that the entity is required by law to maintain the privacy of protected personal information?

- Statement on how individuals may file complaints?

- Effective dates of the notice?

- Are apt actions taken (no later than 30 days) on a request from the individual for access to protected personal information?

- Are approvals obtained from individuals for uses or disclosures of protected health information other than for treatment, expense, or health care processes?

Techniques of Health Data Privacy and Security

The security of data grew continuously as a priority, as the health care industry moved towards greater implementation of digitized health records, and according to proposals of bills that the Congress had already made to facilitate and regulate that transition. Advances in IT very likely, will make it simpler to apply such procedures as audit trials and authorized accessing controls in the future. Though no recommendation has been given to a specific technology solution, there are at least four alternative approaches to increasing data privacy and security that have been proposed by others as being of the potential to be particularly significant in health research. All of the above methods seek to diminish or eliminate the transfer of personal information. These method, their advantages, limits, and feasibility in current scenario are described briefly below.

Privacy-preserving data acquisition and statistical disclosure restraint: Very recently, various techniques have been suggested for modifying or transforming information in a manner so as to preserve privacy while allowing statistical analysis of the data. Normally, such methods reduce the details of representation in order to protect confidential credentials. This, however, leads to a natural exchange in between loss of information and protection of confidentiality because reduction in detailed quantized results in lesser accurate and useable data, and methods that can be followed for their scrutiny. Therefore, an important issue is to maintain maximum usability of data without compromising the primary privacy limitations. Additionally, there is a spectrum of definitions of privacy and its protection in the statistically disclosing limitation and the privacy-preserving data acquisition texts, partially for the varying goals. .

Personal E- health recording devices: The use of personal electronic health record devices has the basic requirement that all individuals possess a personal gadget, such as a personal digital assistant (PDA) or tablet PCs, to record and manage their health information. These devices are intended to be used by individuals to collect all of their health related data onto the device. The infrastructure to implement this privacy-enhancing method exists, but several serious limitations on this technology in health research includes accountability of providing individuals with the mobile devices, the maintenance of these devices, responsibility of bearing the cost of the maintenance, how researchers would request every single individual to permit access to their personal electronic health record device, and the use of personal health recording gadgets would make it highly cumbersome to aggregate data due to the sheer number of sources.

Independent consent management tools: The independent agreement management tool (or infomediary) relies on a third party group a. k. a. health trust to store all of the individual’s health information. When researchers are intent in accessing an individual’s health data for a study, the researchers must contact the health trust (HIPAA, 1999). The concerned authorities then approach the individual and ask whether they are willing to consent to the research. Examples of this technology include Microsoft’s HealthVault and Google Health. Independent consent management facilities allow individuals to make covered consultations for their health information to be available for certain kinds of studies. Some privacy advocates heavily favor such use of technology because according to their perspective it is a way to give patients complete administrator-ship over the access and use of their health information (PPR, 2008).

The use of such technology in health research has a number of huge drawbacks. Firstly, the health trust system becomes a trap vault, in other words, the health trust holds all the individual’s credentials). This creates serious issue of trust and security anomaly, as an individual’s entire health record is stored in a single body. In addition, such firms are presently unregulated by the Privacy Rules of HIPAA, hence, there is no legal federal privacy constraints preventing these units from releasing individuals' data to the people who are ready to pay, and apply no mandatory data security requirements. New laws or regulations making health trusts responsible for security may be necessary, before the general masses are willing to put their trust on such groups to store their personal health credentials. The second big problem to the extensive acceptance of the practice of independently managing consent is the dilemma of availing online secure access to the masses, to view their health records. The companies marketing this technology need to develop a procedure where individuals are able to access their medical information kept by the health trust, without putting any danger on its security and privacy. The biggest problem with using such a system in researches related to health is the inability to ensure the genuineness and truthfulness of responses. As of date there exists no method for the health trusts to give the researchers a guarantee that the information contained in their database is accurate. If still, data is authenticated, such as through the use of digital signing, it is impossible to completely protect the privacy of the individuals' credentials being revealed (NRC, 2003).

Pseudonymization: It is a technique " used to remove the true identities (nominative) of individuals or groups in databases and add pseudo-identities (pseudo-IDs) without direct link to their corresponding real identities" (Claerhout and De Moor, 2005). The benefit of using this technique in health research is that it safeguards individuals' identities while allowing researchers to access and to link personal information across time and place by relying on the pseudo-IDs. Two methods of pseudonymization are the grouped data collection and the interactive data collection

The data are pre-pseudonymized at the source and transported to a trustworthy third party, which converts the pre-pseudonyms data into a last pseudo-ID. Both the last pseudo-ID and charged data are transferred to the data register to be stored and used for research; no information is stored with the provider i. e. the trusted third party. Concealment issues are minimized as researchers can only avail pseudonymized data.

Conclusion

In perspective of health research, privacy means a promise to handle personal information of patients and research participants with complete protection of privacy, inclusive of strong security procedures, limpidity, and responsibility. These commitments apply to all who collect, use, or have access to personal health information of medical cases and research members. Practices of secureness, un-biasedness, and answerability take on high priority in the health research scenario: Health Researchers and other users of health information should clearly confirm how, where from and why personal information is being collected, used, secured, and hence should be subjected to legally enforceable obligations to ensure that personal information is used correctly and securely. Only then will privacy protection help to ensure participants in research and public the trust and confidence in medical research.

References

Aggarwal CC, Yu PS (2008) Privacy-preserving data mining: Models and algorithms. Boston, MA: Kluwer Academic Publishers.

Claerhout B, De Moor GJE. (2005) Privacy protection for clinical and genomic data: The use of privacy enhancing techniques in medicine. Journal of Medical Informatics; 74: 257–265.

Federal Register (February 26, 2001 and December 28, 2000): Part IV Department of Health and Human Services, 45 CFR Parts 160 and 164; Standards for Privacy of Individually Identifiable Health Information; Final Rule

Health Insurance Portability and Accountability Act (1996) Public Law 104-191, 104th Congress

NRC (2003). Who goes there? : Authentication through the lens of privacy. Washington, DC: The National Academies Press.

Nass SJ, Levit LA, Gostin LO, (2009) National Academies Press (US); . Beyond the HIPAA Privacy Rule: Enhancing Privacy, Improving Health through Research; NBK9579

PPR (Patient Privacy Rights). (October 4, 2008) Press release: Microsoft raises the bar for privacy in electronic health record solutions. Accessed August 13, 2008. http://www. patientprivacyrights. org/