The Demand for Technical Safeguards in the Healthcare Sector: a Historical Perspective Enlightens Deliberations about the Future

Emergent Research Forum Paper

Tareq Allan
Dakota State University
tzallan@pluto.dsu.edu

Yong Wang
Dakota State University
yong.wang@dsu.edu

Abstract

This exploratory paper seeks to identify the drivers of demand for technical safeguards in the healthcare sector. Initially, the advent of computing and the increase in computing power were embraced by many healthcare providers without much regard for technical safeguards within systems. However, the advent of media attention when there were breaches of security over patient records and the medical profession's natural regard for patient confidentiality soon developed a consciousness of the need for technical safeguards. The United States of America has been the leading developer of database management in the healthcare sector and it is there that the demand and the advent of technical safeguards have been most advanced. Work at the Rand Corporation, in particular in the 1960s and 1970s, was influential in structuring the discussion and advancing the commitment of the medical profession and the government. This emergent review paper poses two questions: 1. Are there likely to be changes in emphasis in the objectives adopted in development of technical safeguards in the healthcare sector? 2. If there are likely to be changes in the objectives, what might these be?

Keywords

Healthcare, information security, informatics, technical safeguards.

Introduction

Prior to the undertaking of empirical work on security safeguards in the healthcare sector it is important to understand how we arrived at our current situation. Before we can identify the future drivers of innovation in technical safeguards in the healthcare sector, it is necessary to look backwards and seek to identify a pattern in the historical development of drivers. This exploratory review paper is a response to the desire to see the developments of technical safeguards in the healthcare sector in an appropriate historical or evolutionary context. One way to achieve this, is to consider the critical themes and purposes in the historical development of technical safeguards and to consider whether by extrapolation we can make predictions about the future.

Accordingly, the paper is an attempt to discover what might be the future, or make specific predictions, on the basis of the historical development of events and extant trends. What is important today did not just occur in a vacuum, but rather, emerged out of a complex set of historical arrangements. In the case of the technical safeguards in the healthcare sector these complex arrangements involved both the historical development of healthcare records systems (including management systems that relate to accounting data) and the demand of patients (and society at large) for assurances regarding confidentiality and the proper use of databases that accumulate within computer systems. It is reasonable to assume that the historian has a role to play in enlightening us about the emergence of security demands in the healthcare sector and in assisting us to recognize what may be ahead in the sector. Consequently, this paper enters into that space – it seeks to chronicle significant ideas and demands by looking at the work of people who were involved over the last 60 years, assessing the relevance of their contribution to their time and then to our situation today.

The seminal paper of Willis H. Ware was published first as an essay in the Rand 20 first Anniversary Volume, The Rand Corporation, November 1973 (Ware, 1973). The essay was reprinted many times and appears to have been influential in the development of thought about databanks, privacy, the rights of patients and the needs of government and society. There were other papers published about the same time which contributed to the discussion. The ideas in the seminal paper had a gestation period when its author, and other like-minded scholars and practitioners, produced a series of relevant works.

Research questions

The present exploratory emergent research review paper addresses two related research questions:

1. Are there likely to be changes in emphasis in the objectives adopted in development of technical safeguards in the healthcare sector?
2. If there are likely to be changes in the objectives, what might these be?

Early orientation towards technical safeguards

An important organization that was involved in the early thinking around technological safeguards was the American Federation of Information Processing Societies. This Federation brought together professionals in the computing world from all intellectual disciplines and technical practices. The organization grew out of the National Joint Computer Committee, an organization which was formed in 1951, and which held two major annual computer conferences. The origin of this committee was the amalgamation of three "founding societies". These were the Association for Computing Machinery, the American Institute of Electrical Engineers, and the Institute of Radio Engineers. It is apparent that technical/practical persons (those concerned with machinery and engineering) dominated the emerging industry at this stage. In a 1967 conference, it was worth making this very basic point.

With the advent of computer systems that share the resources of the configuration among several users or which address several problems, there is the risk that information from one user (or computer program) will be coupled to another user (or program). The context of early work was relevant regarding the way that systems evolved. The list of topics or concerns that developers held depended on the overall orientation. For example, in many cases, the information in question was a "military classification" and it was vital to maintain the security of the Armed Forces (Ware, 1967, p. 1). In Ware's work the technological field is "military". The focus of his work is narrow in comparison to that which confronts health sector developers today. There is no reference to business or financial concerns, nor is there a reference to the privacy of personal information which has become an issue in the health sector. It is apparent, Ware's paper indicates something of the genesis of concerns about computer users and configurations. Namely, that security concerns (as we would call them today) were the initial stimulus for the development of technological safeguards in complex computer-based systems.

It is interesting to reflect upon the potential for this mental orientation to "color" our thinking in the health sector. At the same conference in 1967, papers refer to other military concerns such as those of the air force users of new computer systems. This conference was the annual conference of the American Federation of Information Processing Societies. Would it be fair to say that in these decades information processing was much a discipline oriented towards military matters? The presence of paper suggests that it was and that there are implications which flow from this.

The implications are twofold. First, the military is a hierarchical organization with the ability for senior people to give orders that will be obeyed by those below them. Consequently, the structures which can evolve naturally there for computer security systems will be essentially "top-down" – they will be about control from the center of the organization in accordance with broad overall purposes. This contrasts with the situation in the healthcare sector where patients believe that they have rights in relation to the data held about themselves (medical records and statistical information) and consequently the control mechanism which they would envisage derives from their position as patients, and we may characterize it as "bottom-up".

Second, compliance within the military is much less of an issue than it is within the civilian population. The military is trained to obey orders and there are heavy sanctions upon those who transgress. However,

in the civilian world – which is the world of the healthcare professionals and their patients – there is no such acceptance of authority. Decision-making must proceed by cooperation and understanding.

It is apparent that these twofold concerns work together to generate in the healthcare sector a business environment which is dramatically in contrast with the military sector. There is a sense in which the healthcare sector in the area of computer security has been attempting to overcome the origins of the computer security discipline.

The present paper considers two aspects of the healthcare sector's concern with technical safeguards: formal policies and procedures; and, education and training.

The march of policy

The policy environment in the healthcare sector continues to evolve. Organizations are being transformed as new ideas are brought to fruition and healthcare professionals face the development of new management practices around data security and technology (Flynn, Mathis, Jackson, & Valentine, 2016; Mastrian & McGonigle, 2017; Sims, Sauser, & Bias, 2016; Skurka, 2017). The foundation for all of this is the rapid development of health law, particularly in the United States of America (Cohen, Hoffman, & Sage, 2017). It is probably true to say that the technology initiatives, such as the raft of devices directed at improved healthcare outcomes and the role of big data in public health, are the public side of information technology in healthcare (Garets & Garets, 2016; Kshetri, 2016; Pesch-Cronin & Marion, 2016). Critical protection of the infrastructure – both hardware and software – is something which only as seen by information technology professionals. Health professionals are unlikely to get excited about innovation here. These developments can sometimes produce diverse requirements for policy initiatives – but they seldom (if ever) challenge the basic goals and objectives for information technology in the security fields.

The advent of mobile devices, cloud computing systems, and new applications in the healthcare sector have created a further distinct set of challenges for those involved in data/information security. Those involved at all levels in the system with the maintenance of policy need to be aware of this and to respond (Bhatt & Peddoju, 2017).

The demand for education and training

The challenge of education and training in relation to patient records became apparent in the United States of America, particularly in the 1960s (Weed, 1969). By the turn-of-the-century there was much more sophistication in relation to the electronic patient records management (see for example, Chao, Hsu, & Miaou, 2002). There was also a clear focus on ethical issues in relation to the management of patient records (Kluge, 2001). A part of this is the desire to involve patients in the medical/administrative decision-making concerning their records (Powell, Fitton, & Fitton, 2006). There are many guidelines provided by authorities and specialists for use in training in security matters within the healthcare sector (International Association for Healthcare Security and Safety., 2002; Meserve & International Association for Healthcare Security and Safety., 2004; Meserve & Williams, 2007, 2010; Meserve, Williams, & International Association for Healthcare Security and Safety., 2007). A quick review of these reveals that they have certain uniformity with regards to the overall purpose that they portend. The challenges which are identified in the training materials relate to the difficulties of pedagogy when you work in an environment which displays cultural difference, including language barriers. Nurses, for example, trained in the United Kingdom or the United States come to their work with a distinctly different set of cultural expectations than nurses trained in some of the Asian countries. Such cultural differences are important because patient outcomes can be influenced by them and this includes how nurses manage electronic medical records (Furukawa, Raghu, & Shao, 2010). This has implications for all training activities and for the implementation of policies regarding database security

Conclusion

The rapidity of change within the information technology sector is a matter of perception. Likewise, the rate of developments in the health sector is also perceived in different ways by different people. With that caveat, nevertheless, it is remarkable that there is been so much progress with the management of health records over such a few decades. Although it appears to be clear that the technical advances were in many

cases pioneered in the United States of America, the United Kingdom and other countries have also contributed to initiatives. The development of strategies and practices with regard to technical safeguards in the health sector, drawing as they do upon the internationalization of medicine and information technology, are remarkably global in their application.

The harmonization of policy, and the rapid adoption of new policies and standards, is a relatively easy achievement for health authorities in different countries. A more challenging issue, is the implementation of those policies as this requires the education and training of the health sector workforce. It is not just the senior managers or clinicians in the health sector that have to be involved in this – it applies to every discipline and sub-discipline of medicine and surgery, to all the mental health disciplines, to the laboratory sector, to the recuperation sector, and to a myriad of support workers. Education and training resources in the health sector are limited by financial constraints and the information technology needs must compete for funding within the sector. There is also the challenge of engaging a technology literate workforce. The technological culture which is found within the United States and the United Kingdom is not universally the culture of other countries. An enquiry into culture is beyond the scope of the present paper but it must be acknowledged that the cultural perspective may be important in addressing the objectives of the present exploratory paper.

For the future, it is difficult to see anything other than refinements of the current strategies. The technological advances will continue but the theory (the foundation of policy and the justification of policy writ large) will remain largely undisturbed. It is apparently agreed by all stakeholders that it is important to maintain public confidence in the healthcare sector. There is also comprehensive support for the rights currently afforded to patients. Thus, the broad goals of policy, which have emerged in the last few decades, are agreed. Can we predict the *technological* advances which will be significant in the healthcare system? There will be further increases in the capacity to process databases and to minimize the impact of the hardware on users. There is an increasing use of voice-activated recording devices in the medical profession and these have improved dramatically just in the last two decades. We can expect this trend to continue. We can also expect that there will be a greater amount of automatic analysis and advisory facilities developed for the medical profession. In contrast to these things, the technical safeguards in the health care industry will become more hidden. There will be greater sophistication both in terms of hardware and software, but there will be less to see – success in relation to technical safeguards is marked by invisibility.

REFERENCES

Bhatt, Chintan M., & Peddoju, S. K. (2017). Cloud computing systems and applications in healthcare. Hershey, PA: IGI Global.

Chao, H. M., Hsu, C. M., & Miaou, S. G. (2002). A data-hiding technique with authentication, integration, and confidentiality for electronic patient records. IEEE Trans Inf Technol Biomed, 6(1), 46-53.

Cohen, I. Glenn, Hoffman, Allison, & Sage, William M. (2017). The Oxford handbook of U. S. Health Law. New York, NY: Oxford University Press.

Flynn, Walter J., Mathis, Robert L., Jackson, John H., & Valentine, Sean. (2016). Healthcare human resource management. Boston, MA, USA: Cengage Learning.

Furukawa, M. F., Raghu, T. S., & Shao, B. B. (2010). Electronic Medical Records, Nurse Staffing, and Nurse-Sensitive Patient Outcomes: Evidence From the National Database of Nursing Quality Indicators. Medical Care Research Review.

Garets, David E., & Garets, Claire McCarthy. (2016). The journey never ends : technology's role in helping perfect health care outcomes. Boca Raton: CRC Press, Taylor & Francis Group.

International Association for Healthcare Security and Safety. (2002). Basic training manual and study guide for healthcare security officers : a program of the International Association for Healthcare Security and Safety. Lombard, Ill.: International Association for Healthcare Security and Safety (IAHSS).

Kluge, Eike-Henner W. (2001). The ethics of electronic patient records. New York: P. Lang.

Kshetri, Nir. (2016). Big data's big potential in developing economies : impact on agriculture, health and environmental security. Boston, MA: CABI.

Mastrian, Kathleen Garver, & McGonigle, Dee. (2017). Informatics for health professionals. Burlington, MA: Jones & Bartlett Learning.

Meserve, Evelyn, & International Association for Healthcare Security and Safety. (2004). Healthcare security supervisory training manual and study guide. Glendale Heights, Ill.: International Association for Healthcare Security and Safety.

Meserve, Evelyn, & Williams, Nancy B. (2007). Basic training manual for healthcare security officers. Gendale Heights, IL: International Association for Healthcare Security and Safety.

Meserve, Evelyn, & Williams, Nancy B. (2010). Basic training manual for healthcare security officers. Gendale Heights, IL: International Association for Healthcare Security and Safety.

Meserve, Evelyn, Williams, Nancy B., & International Association for Healthcare Security and Safety. (2007). Supervisor : training manual for healthcare security personnel. Gendale Heights, IL: International Association for Healthcare Security and Safety.

Pesch-Cronin, Kelley A., & Marion, Nancy E. (2016). Critical infrastructure protection, risk management, and resilience : a policy perspective. Boca Raton, FL: Taylor & Francis Group.

Powell, J., Fitton, R., & Fitton, C. (2006). Sharing electronic health records: the patient view. Inform Prim Care, 14(1), 55-57.

Sims, Ronald R., Sauser, William I., & Bias, Sheri. (2016). Transforming government organizations : fresh ideas and examples from the field. Charlotte, NC: Information Age Publishing, Inc.

Skurka, Margaret Flettre. (2017). Health information management : principles and organization for health information services. Hoboken, New Jersey: John Wiley & Sons, Inc.

Ware, Willis H. (1967). Security and privacy in computer systems. Paper presented at the Proceedings of the April 18-20, 1967, spring joint computer conference.

Ware, Willis H. (1973). Data Banks, Privacy, and Society. Available at https://www.rand.org/content/dam/rand/pubs/papers/2008/P5131.pdf. Santa Monica, CA: The Rand Corporation.

Weed, Lawrence Leonard. (1969). Medical records, medical education, and patient care: the problem-oriented record as a basic tool: Cleveland: Press of Case Western Reserve University.