NORTHWESTERN
UNIVERSITY

Criticism Paper

Kevin Scharnhorst

A critical review of an article from Noam H. Arzt, PhD entitled “Rising to the Challenge: Strategies for the new Healthcare Enterprise” written in 2003.

MMI 407 – Legal, Ethical
& Social Issues in
Medical Informatics

Fall 2010

Northwestern University

Table of Contents

Criticism of
"Rising to the Challenge: Strategies for the new Healthcare Enterprise"
by Noam H. Arzt, PhD

The purpose of this project paper is to criticize the titled article and to point out weakness of thought and to review the comprehensiveness of coverage at the time the article was written. I will also point out changes around issues identified by the article since the time of its writing.

Introduction

The author starts the article off badly with a vaguely broad overview of respondents' answers to a survey covering three questions about security concerns revolving around access to healthcare information. The textual reference to these concerns is hard to follow and compares concerns spanning from 2001 and 2002. The reader is able to get the general idea that concerns to information security is on the rise over a two year period and across three different areas, but this information would be better communicated through a visual aid such as the one in table 1. Another lacking detail that could have been mentioned are examples of each. Examples would help frame the concerns better for the reader.

Issue/Question	2001	2002
1) Unathorized access a major concern	59%	62%
2) Inappropriate access from within the institution	55%	65%
3) Violations of data security practices	50%	58%

Table 1

Another fault of the article is that the author offers no contextual reference as to events happening at the current time that might contribute to the respondents' answers. We know that at the time of the writing, in 2003, that the Health Insurance Portability and Accountability

Act (HIPAA) existed for 7 years. By 2003, HIPAA was maturing. The article was written by the summer of 2003, and in April, of that same year, the Privacy Rule was enacted to HIPAA. Under the Privacy Rule, protections were put into place to regulate the exchange of information between healthcare organizations. It covers medical records, payment histories and provides guidelines around the use of Protected Health Information (PHI). Deidentified data ("Safe Harbor"), Limited Data Sets, "Minimum Necessary" rule, Business Associate Agreements (BAAs) were all components required in the exchange of information to protect PHI. Any violations around the protections offered through the Privacy Rule could be brought for appeal to the Department of Health and Human Services Office for Civil Rights.

In February, of the same year the article was written, the Security Rule was enacted under HIPAA. This rule put into place protections guaranteeing the safeguards of PHI around the handling or exchange of information. The Security Rule specifically required that healthcare information exchanges be protected physically, administratively, and technically. The means by which it is acceptable to share PHI became pretty clear cut under this provision. In order to share PHI, an organization or individual has to meet 6 conditions. The first three are used, being that the information is be used for purposes involved to coordinate treatment, payment or operational functions (together referred to as TPO). Fourth, the information is provided by order of the court or for public health safety. Fifth, the information is being released to the requestor with prior written authorization from the patient. Lastly, PHI can be released through a waiver of patient authorization issued by an institutional review board or privacy committee. (Lindgren, 2010) Through these protections of information, I think the level of concern may have been lower of the respondents questioned. At the time of the article's writing it was too early to tell the effects these protections might have had on their individual concerns.

Given the last two enactments mentioned, there was no doubt concern over inappropriate access to information across the three areas mentioned by the author. It is clear that the industry was aware and through proper governmental channels these two regulations sought to close the gaps from which security concerns stemmed. The article would have been strengthened by mentioning these developments. As enforcement was put in place, I would expect the level of concern to decrease as subsequent years passed.

To further weaken the lead in to the rest of the article, the author almost makes excuses or justifications for why security is lacking and seems to foster this mentality rather than challenge Healthcare Enterprises to "up the ante". I'm disappointed by what the author suggests when he said, "….information security was mostly a game of risk and insurance: you determined what your level of risk was based on a threat analysis and judged how likely and how damaging the threats might be if they occurred. You then developed mitigating strategies and decided if the cost of mitigating was warranted based on the perceived risk of taking no action". This whole notion supports the whole idea of reactionary thinking instead of pro-activeness. Perhaps a naïve thought, but I believe medical professionals were aware of the sensitivity to medical information long before the prospect of storing it digitally. Most would install physical safeguards to protect printed forms of medical information.

The author does give a brief history of the network topology that existed in early computing days. The idea being, that most were private and disconnected. The author points out that privacy and security concerns really began to heighten as the internet became more prevalent. I agree on that point, however, by 2003, it was “too little, too late”. Most businesses were engaged in transacting business through electronic commerce and the number of healthcare organizations with Electronic Medical Record (EMR) systems installed was heightening as well. According to one source that reported on number of vendor installs by year, in 1998 there were roughly 3,000 EMR vendor installations in existence. In 2003, that number had grown to more than 16,000. (NASBHC, 2005) The author fails to provide any point of reference as to the prevalence of the systems that make this information electronically available. Such reference would underscore the daunting nature of the challenge suggested by the article’s title.

The main points

The idea of risks and tradeoffs serves as the undertone and structure for rest of the article. He outlines 12 main tradeoffs for consideration, followed by 5 recommendations. We will dive into detail on all of these points as the paper is further criticized.

Ease of Use

The author’s statement that “users often feel security implementations interfere with their ability to do their jobs effectively” is likely a matter of opinion. Given points already covered and knowing that EMR applications were becoming quite common across hospital and ambulatory settings, I think security was probably already a concern. The sensitivity of the information stored in the EMR is realized. Professional healthcare staff realize that precautionary measure taken afford better confidentiality and patient safety. Knowing this, the inconveniences incurred offer more benefit than hindrance. With the information being electronic and intangible, it also becomes easier to share and harder to restrict. Passwords and role based security becomes a tool for restricting, auditing and controlling the access of information.

In consideration for the author's approach, he may be suggesting that "ease of use" needs to be considered in order to get broader acceptance with users. The Privacy Rule would not extend leniency to allow an organization to consider tradeoffs to relax or remove technical safeguards. However, the language of the regulation offers much to be interpreted by the organization. The Centers for Medicare & Medicaid Services (CMS) offers an educational resource to help advise on HIPAA security topics. The CMS material goes into great detail on the specific safeguards required under the Privacy Rule. Regarding technical safeguards they offer that "the Security Rule does not require specific technology solutions……there are many technical security tools, products, and solutions that a covered entity may select. Determining which security measure to implement is a decision that covered entities must make based on what is reasonable and appropriate for the specific organization given their own unique characteristics. (HIPAA Security Series, 2007) "Reasonable and appropriate" then become the key. An organization can meet that definition while also seeking to find a solution that is easy to use.

Locations

As with "ease of use" falling under technical safeguards, location could be considered a physical safeguard. From the same CMS educational material it clarifies physical safeguards as "physical measures, policies, and procedures to protect a covered entity's electronic information systems and related building and equipment, from natural and environmental hazards and unauthorized intrusion". Restricting access by physical location then would be a necessary precaution for an organization. The CMS further provides that "when evaluating and implementing these standards, a covered entity must consider all physical access to EPHI. This must extend outside of an actual office, and could include workforce members' homes or other physical locations where they access EPHI." (HIPAA Security Series, 2007) Examples mentioned of physical safeguards include "locked doors, signs warnings of restricted areas, surveillance cameras, alarms. Property controls such as property control tags, engraving on equipment. Personnel controls such as identification badges, visitor badges and/or escorts for large offices." (HIPAA Security Series, 2007) In most of the examples shared, these are controls that must be insured within organizational facilities. Remote locations would relinquish the control that an organization would otherwise have in enforcing these physical safeguards.

Cost and Funding

The author's point on the cost to an organization is relevant. I agree on the point that some deeper expenses are hard to see and present in the total cost picture. He alludes to the point that costs will be more if security precautions are in place when he says "all it takes is one disaster for many institutions to open the checkbook". This supports the old adage by Benjamin Franklin that "an ounce of prevention is worth a pound of cure". As an example of a resulting cost of not having security safeguards in place, imagine a scenario where "a hacker were able to gain access to a physician practice's computer system that contained patient information, the physician practice would have to inform all patients and the Department of Health and Human Services (HHS) of the breach. In some cases, the physician practice would also need to notify the media”. (AMA FAQ, 2010) The research, public relations and action plan to identify and remedy the situation would be very costly to the institution. These breach notification requirements did not apply at the time the article was written, but The Health Information Technology for Economic and Clinical Health (HITECH) Act requires them today

However, I would further argue, that security doesn’t have to be expensive. The “ounce of prevention” could be as simple as encrypting all electronic personal health information (EPHI). A physician practice, such as our previous example, could avoid the extensive notification requirements otherwise required by HITECH in the event of a security breach through this. Further, costs are avoided and EPHI is protected along the way. Covered entities and their business associates are not under the same notification requirements. The AMA has commented on the costs of encryption in saying that it “can be expensive, but it doesn’t have to be. Some encryption programs are available at no cost. Microsoft EFS, for example, is shipped as a part of the Windows operating system. Microsoft also provides whole-disk encryption on Windows 7 systems with a program called BitLocker™ Drive Encryption. Other programs, such as TrueCrypt®, may be downloaded and installed for free. At the other extreme, encryption devices known as hardware security modules (HSMs) can be quite expensive. The choice you make depends on many factors, including encryption strength, speed, available technical support and ease of use.” (AMA FAQ, 2010) This supports again the idea of “ease of use”. Security does not have to be complicated and the organization, again, can choose a combination of solutions that work for them.

Although encryption is only one example of costs, the idea is that institutions employ measures that will protect themselves and the lives they are involved in caring for. In doing so, patient safety is ensured and costs reduced.

Funding becomes less of a concern as we fast forward past the time of this article to present day. The need to expand electronic medical records is recognized and financial incentives are being offered to healthcare institutions that move their organizations towards this direction early under HITECH's "meaningful use" objectives. CMS helped to define the incentives, but essentially there is $27 billion dollars available over a 10 year period. The coined phrase for "meaningful use" is meant to tie back to organizations implementation of EMRs in a meaningful way that will contribute to significant improvements in care processes and outcomes. Also within the objectives are requirements around the security and technical implementation for organizations to implement successfully and within compliance.

Given these incentives, the author's point on funding becomes a mute one. If organizations still choose to stay behind and not convert to electronic medical records, the incentives turn into fines if they have not implemented past 2015. So these will be financial costs for non-compliance.

Organizational Flux

The author points out the vast array of changes that had taken place in the city he lived for more than 25 years. There is not much to disagree with here. This trend seems to cycle and be a part of the healthcare industries culture. Today, the economy struggles. Larger hospitals are acquiring local provider practices to increase their vertical market share. Institutions churn in staff positions. This will likely never change. To combat this, organizations will be required to stay current with technology and security concerns and forward looking in their solutions so that they can remain agile and adapt as required. The landscape has evolved a great deal since the time the author wrote the article. The Internet has made possible extended networks that enable providers, payers, pharmacies, etc . to exchange information between them.   These information exchanges are referred to as Regional Health Information Organizations (RHIO) or Health Information Exchanges (HIEs). One of the primary benefits is that in the achieved collaboration it accomplishes better continuity of care for patients. As exchanges continue to evolve, institutions will be required to be more nimble in changing to adapt their policies, procedures and technologies in a secure manner to remain compliant with security regulations and practices.

Furthermore, as the physical make up of organizations change, under HIPAA, another consideration is the organization of the executive leadership. Amongst the normal chief officers that exist in an enterprise, we should also see both a security and privacy officer under the “new enterprise”. The author mentions the CEO under the agenda for the “new enterprise”, but gives no reference to the Chief Privacy and Security officers, but both are required under the HIPAA Privacy Rule. These two roles will play a vital role in forming the policies and procedures that the author recommends in his agenda. They will in essence contribute in helping remove the flux within healthcare organizations and provide leadership in being more nimble and help drive organizations in the right direction.

Consumerism, New Services and the Tangled Web.

The author suggests that organizations must decide to "enter the fray or stay on the sidelines" with consumers demand for easy access to information. I would argue that even in 2003 there was not much of a choice. Organizations that have made the choice not to go to the web will have already been left behind. It was then, and is even more so now, how business is done in this day and age of technology. I think consumers have come to expect access to information and services on the web and the various forms of electronic devices that are available. I would argue that the author, himself, is a bit outdated if he thought that this demand for information was just starting in 2003.

Further in the article, he touches on the various sources of information that we have to keep up with and process. He acknowledges "the pressure of constant connectedness has reduced our attention span as we juggle pagers, PDAs, cell phones, laptops and our commitments".   With that statement, he recognizes the numerous options of information for which information can be targeted too. All of the mentioned devices have capabilities to access information from the web. With that access, organizations can choose the type of information that can be distributed and the types of services that will be offered. To cut down on the information overflow and decreased attention spans mentioned in the article, healthcare organizations can help consolidate the amount of information to process. As one example, consider the Personal Health Record (PHR). The PHR can be maintained by individuals and that can reduce repeat needs for individuals to update their physician, hospital or pharmacy with the same redundant information. With the PHR, that information could be updated in one place by the individual and then shared with all providers that require it. The providers would update the record as well with record information as the patient was cared for by them. The end result is an updated consolidated view of information.

These type of electronic records offer many benefits. To mention a few, the U.S. Department of Health & Human Services has a website which promotes private and secure electronic health information exchanges through meaningful use. They list the below three benefits: (Electronic Health Records and Meaningful Use, 2010)

- Complete and accurate information. With electronic health records, providers have the information they need to provide the best possible care. Providers will know more about their patients and their health history before they walk into the examination room.
- Better access to information. Electronic health records facilitate greater access to the information providers need to diagnose health problems earlier and improve the health outcomes of their patients. Electronic health records also allow information to be shared more easily among doctors' offices, hospitals, and across health systems, leading to better coordination of care.
- Better access to information. Electronic health records facilitate greater access to the information providers need to diagnose health problems earlier and improve the health outcomes of their patients. Electronic health records also allow information to be shared more easily among doctors' offices, hospitals, and across health systems, leading to better coordination of care.

These mentioned benefits support the cause to further move toward secure electronic records and information exchanges. The author discounts the idea of RHIOs or HIEs, however at the time the article was written, advances were being made in this area. Although plagued with challenges, I think the real challenge for the "new enterprise" is to combine these smaller information exchanges into the National Health Information Network (NHIN) framework. He fails to even mention the NHIN, but the idea was around for at least three decades at the time of the writing. As exchanges become more standardized, many of the hurdles or “tradeoffs” mentioned in the article will be overcome and HIEs, RHIOS and NHIN become achievable. Vendor solutions are popping up all over the place to rise to the challenge presented with information exchanges. Platforms based on service oriented architectures seem to be prevailing as the common solution. Platforms that remain agnostic to technologies will have the best chance for success. Organizations such as the Agency for Healthcare Research and Quality (AHRQ) are forming the foundation for a nationalized data stewardship. All the mentioned players are coming culminating together to overcome current challenges.

The legal framework that will govern compliance will also help adoption and implementation of technologies and security safeguards to be successful in offering new services targeted for consumption on distributed networks such as the web.

Technology Transfer and Intellectual Property

The author mentions intellectual property (IP) as a concern in reference to advances in biomedical research, but fails to go into any detail. As with the rest of the “tradeoffs” mentioned, he throws out buzz words, but fails to demonstrate any depth of understanding about them and further lacks any recommendations to overcome them. There are five legal protections under the IP legal framework that can assist individuals in organizations. Those include Copyright, Trademark, Patent, Trade Secret and Contractual protections. I would have expected even a light overview of some of these tools and specifics on how the “new enterprise” might embrace them to protect both individuals and clinician-researchers and their institutions.

Recommendations

In all fairness, the author's recommendations does seek to focus the reader in a forward looking manner even though the introduction seemed to make excuses for not doing so. The advice in his conclusion is centered on having a plan on four things; think about policies and procedures, stay current on hardware, move towards the web and be concerned with portable devices. These are no doubt important in advancing readers to think forward. However, I think the article overall was weak and shallow in its coverage of the points shared. His recommendations do not really solve any of the challenges or "tradeoffs" that were pointed out, beyond getting individuals thinking on them. The "tradeoffs" and recommendations lack substance and *if* provoked to act, the reader is left wondering how. As pointed out already, in 2003, EMRs were experiencing an explosion of growth. This fact is the most concerning. The author's suggestions do nothing to calm that concern. With so many installations, how do you wrap your arms around the problem if proactive thought was not invested before hand? So, my overall impression in reading the concluded advice is, so what, what difference will these make on the challenges pointed out.

Conclusion

The article has a strong title! Most individuals rise to challenge. We grow from adversity and become stronger after overcoming it. The title speaks almost as a "call to arms", yet in conclusion, I am left with the desire retreat in defeat. A noble leader would arm his soldiers with confidence and tools to be successful in battle. Detail direction is lacking throughout all of what was covered by the author. Consider yourself blind folded on the battlefield and the authors “tradeoffs” as intelligence gathered to identify strategically placed land mines by the enemy. Would the detail given instill confidence enough to step forward? If so, would the recommendations offered leave you knowing where to step to avoid the next lethal pitfall? I’m left scared and apprehensive to advance even one step forward in battle.

The legal framework and points added in this criticism offer the detail that is lacking to help the reader know what the challenges are in forming the “new Healthcare Enterprise” and offer the direction needed to lay the needed foundation for a successful implementation of secure health information exchange. We have touched on new developments since the writing of the article that can serve to motivate the ranks within organizations’ further. If the article were to be republished these developments that were underway at the time of the writing and those that have happened since would offer greater confidence that the goal is achievable. The government is doing a lot to support the healthcare industry in advancing it forward in the right direction. Following the battle analogy, the government in essence is acting as a supporting battle alliance to strengthen the battle front against the challenges it is faced with. They are offering a map to successfully navigate the mine fields.

Overall, these points as covered, would lead to a strong motivating force to empower individuals and organizations with the information and tools necessary to succeed. Empowered with better direction, confidence would grow and together we would charge forward on the battlefield and arrive victoriously united together. All involved would be edified through their contribution to conquer the challenge!

References

Arzt, N. H., PhD. (2003). Rising to the Challenge: Strategies for the New Healthcare Enterprise. [Editorial]. *Journal of Healthcare Information Management, Vol. 17, No. 3*, 9-11. Retrieved October 25, 2010 from the World Wide Web: http://www.nogginlabs.com/blackboard/med_inf_407_10_51_winter09/6criticism%20project%20examples.pdf.

Electronic Health Records and Meaningful Use. (2010). Retrieved October 29, 2010 from U.S. Department of Health and Human Services, HHS: http://healthit.hhs.gov/portal/server.pt?open=512&objid=2996&mode=2.

Health Information Technology (HIT) and Electronic Medical Records (EMRs) . (2005). Retrieved October 25, 2010 from NASBHC.org, National Assembly on School-Based Health Care: http://www.nasbhc.org/atf/cf/%7bcd9949f2-2761-42fb-bc7a-cee165c701d9%7d/ta_hit_history%20of%20emr.pdf.

HIPAA Security Series. (2007). Retrieved October 28, 2010 from Centers for Medicare and Medicaid Services, Department of Health and Human Services: http://www.hhs.gov/ocr/privacy/hipaa/administrative/.../techsafeguards.pdf.

HIPAA Security Rule: Frequently Asked Questions regarding encryption of personal health information. (2010). Retrieved October 28, 2010 from American Medical Association, American Medical Association: http://www.ama-assn.org/ama1/pub/upload/mm/368/hipaa-phi-encryption.pdf.

Lindgren, K. (Professor). (2010). *MMI 407 Class Lecture Content*. Northwestern University.