An Integrative Framework for Achieving HIPAA-Compliance for Healthcare Information Systems

Nilmini Wickramasinghe, Center for the Management of Medical Technology (CMMT), Illinois Institute of Technology, 565 West Adam Street, Suite 406, Chicago, IL 60661, USA; E-mail: nilmini@stuart.iit.edu

Rajeev K. Bali, Knowledge Management for Healthcare (KARMAH) Research Subgroup, Biomedical Computing and Engineering Technologies (BIO-CORE) Applied Research Group, Coventry University, UK

ABSTRACT

*Currently the Healthcare industry globally is contending with relentless pressures to lower costs while maintaining and increasing the quality of service. Robust Healthcare Information Systems (HCIS) become critical to enabling healthcare organizations address these challenges. In this paper, we propose an integrative framework for HIPAA compliant, I*IQ HCIS. We base this framework on an integration of the requirements for HIPAA compliance, the principles of Information Integrity (I*I), as well as the healthcare quality aims (Q) set forth by the Committee on the Quality of Healthcare in America (American Institute of Medicine, 2001). The power of this framework is that, while it has been developed taking into account critical issues pertaining to security in the US healthcare environment it is as relevant in any healthcare system. To illustrate its universality we discuss the appropriateness of this system in the UK NHS environment as well.*

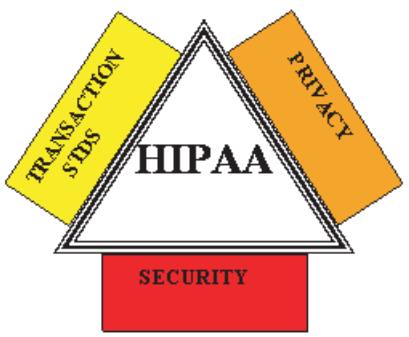
Keywords: HIPAA, Information Integrity, healthcare, healthcare information systems (HCIS), framework, privacy, security, standards, quality, NHS

1.0 THE HIPAA TRIANGLE

In the US, HIPAA (the Health Insurance, Portability and Accountability Act) focuses on three key elements; namely, security, privacy and standards for electronic submissions and exchange of healthcare information (American Institute of Medicine, 2001; HIPPA, 2001; Moore and Wesson, 2002). It is useful to conceptualize this as a triangle (figure 1) which highlights the fundamental elements of the HIPAA regulation; namely, security, transaction standards and privacy.

- **Security:** According to HIPAA, a number of security criteria must be met by all electronic healthcare transactions. Some of these criteria directly affect how healthcare systems can be accessed and interacted with by the users of healthcare information systems. Essentially, these security criteria fall into 3 main categories; namely administrative, physical and technical.

Figure 1. HIPAA triangle



- **Transaction Standards: The Standards for electronic health information transactions cover** certain electronic health transactions, including claims, enrollment, eligibility, payment, and co-ordination of benefits.
- **Privacy:** The final element of the HIPAA triangle deals with ensuring the **privacy of healthcare information.** Specifically, the Federal Register (Vol. 67, No. 157) details all the rules that must be adhered to with respect to privacy. The purpose of these rules is to maintain strong protections for the privacy of individually identifiable health information, addressing the unintended negative effects of the privacy requirements on healthcare quality or access to healthcare, and relieving unintended administrative burdens created by the privacy requirements. Thus, theses privacy requirements cover uses and disclosures of treatment and payment information and create national standards to protect individuals' medical records and other personal health information.

2.0 INFORMATION PRODUCERS, CONSUMERS AND INFORMATION FLOWS WITHIN THE HEALTHCARE SYSTEM

In order to fully capture the flows of information it is necessary to first identify the primary producers and consumers of data and information within the healthcare system. At the center of the information flows is the HCIS because not only does it connect the key players within the healthcare system in an efficient and effective manner but also it forms the central repository for key information such as patient medical records, billing, and treatment details. Hence, the HCIS provides the foundation for supporting the information flows and decision making throughout the healthcare system.

Healthcare procedures such as medical diagnostics, treatment decisions and consequent effecting of these decisions, prevention, communication and equipment usage can be thought of as iatric in nature (Perper, 1994). Integral to these iatric procedures is the generating and processing of information (Moore and Wesson, 2002). The patient naturally provides key information at the time of a clinical visit or other interaction with his/her provider. Such a visit also generates other information including insurance information, medical history, and treatment protocols (if applicable) which must satisfy regulatory requirements, payer directives and, obviously, the healthcare organization's informational needs. Thus, we see that from a single intervention many forms and types of information are captured, generated and then disseminated throughout the healthcare system. All this information and its flows must satisfy some common integrity characteristics such as accuracy, consistency, reliability, completeness, usefulness, usability and manipulability. Consequently, generating a level of trust and confidence in the information's content and processes. Since the information flows across various organizational boundaries, the challenge of ensuring information integrity is further compounded because any integrity problems will propagate with ripple effects following the same trajectory as the information itself. Given the high degree of inter-relatedness between the various players, the consequences of poor quality information (such as the cost of information integrity problems) are multiplied and far reaching. This highlights the need for robust, well designed and well managed HCIS (Applegate et al., 1986; Stegwee and Spil, 2001). Such a perspective

should not be limited to new systems, but rather, equally and perhaps of even more importance, should be applied to existing systems as well.

3.0 INFORMATION INTEGRITY AND QUALITY (I*IQ)

Given the critical role of information both within and between the information produces and consumers in healthcare (Chandra et al., 1995), it is imperative then that the information flowing both within the HCIS and between the key participants in the healthcare system must exhibit both the attributes and dimensions of the information integrity construct as well as satisfy the healthcare quality aims. Specifically, the information should display the attributes of accuracy, consistency, and reliability of content and processes as well as the dimensions of usefulness, completeness, manipulability and usability (Moore and Wesson, 2002; Chandra et al., 1995; Geisler et al., 2003).

3.1 Information Integrity

Information integrity is an emerging area that is 'not just about engineering the right properties of information but it also includes sensitivity to the context in which information is used and the purpose for its usage' (Geisler et al., 2003 p5; MAndke et al., 2003). More specifically it encompasses the accuracy, consistency, and reliability of the information content, process, and system. By focusing on the privacy, security and standards aspects of healthcare information, it would appear that HIPAA implicitly assumes certain characteristics of this information product such as its accuracy and reliability. However, in practice this may not always be the case, and from the perspective of the healthcare organization it is not sufficient to be HIPAA compliant, rather it must also ensure the information product satisfies the principles of Information Integrity (I*I) standards. Implicit in taking an Information Integrity perspective is the shift from viewing information as a byproduct to viewing it as an essential product (Huang et al., 1999). This requires following four key principles; namely that the information must 1) meet the consumers information needs 2) be the product of a well defined information production process 3) be managed by taking a life-cycle approach and 4) be managed and continually assessed vis-à-vis the integrity of the processes and the resultant information [ibid]. In order to actualize this I*I perspective, healthcare organizations then need to implement specific protocols.

3.2 Healthcare Quality Aims

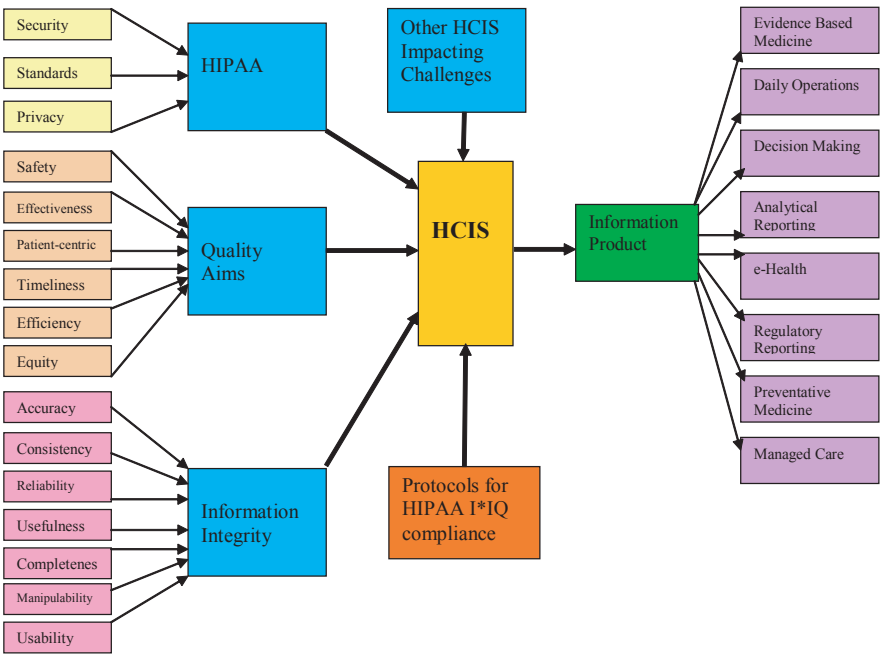
In the final report of the Committee on the Quality of Health Care in America (American Institute of Medicine, 2001), it was noted that improving patient care is integrally linked to providing high quality healthcare. Furthermore, in order to achieve a high quality of healthcare the committee identified six key quality aims; namely, 1) healthcare should be safe – avoiding injuries to patients from the care that is intended to help them, 2) effective - providing services based on scientific knowledge to all who could benefit and refraining from providing services to those who will not benefit (i.e. avoiding under use and overuse), 3) patient-centered – providing care that is respectful of and responsive to individual patient preferences, needs, and values and ensuring that patient values guide all clinical decisions, 4) timely – reducing waiting and sometimes harmful delays for both those receiving care and those who give care, 5) efficient - avoiding waste and 6) equitable – providing care that doesn't vary in quality based on personal characteristics. It is obvious that these quality aims can only be negatively impacted by poor information quality, flow and integrity. Conversely, a higher quality, flow and integrity of information will positively impact these quality aims by helping to reduce the large number of medical errors that currently permeate the healthcare system (Moore and Wesson, 2002; Chandra et al., 1995; Geisler et al., 2003). What becomes critical then is to incorporate these quality aims into the manufacturing of the information product so that the output is quality information. This requires the establishment of an information quality program which serves to: 1) articulate an information quality vision in healthcare business terms, 2) establish central responsibilities for information quality within the information product manufacturing processes, 3) educate the producers and consumers of information on information quality issues and 4) institutionalize and continuously evaluate and develop new information quality skills (Huang et al., 1999).

4.0 PROPOSED FRAMEWORK

Information systems/information technologies (IS/IT) are becoming key enablers and strategic necessities for organizations irrespective of their business sector (Haag et al. 2004; Scott Morton, 1991; Thorne and Smith, 2000). Hence, it should come as no surprise to expect HCIS to play a similar role for healthcare organizations; in particular, they should be viewed as key enablers for healthcare to meet the challenges with which healthcare is currently grappling. In order to systematically maximize and facilitate the full potential of HCIS to enable healthcare organizations cope with today's challenges, it is important to have a guiding to facilitate the design and management of robust HCIS. We propose the following integrative framework as a potential candidate.

The proposed framework integrates the key challenges of 1) the HIPAA triangle, 2) the six healthcare quality aims and 3) the core principles of information integrity currently facing all healthcare organizations in the US (Wickramasinghe

*Figure 2. An Integrative Framework for HIPAA I*IQ HCIS (adapted from Wickramaisnghe, 2006)*



and Sharma, 2005). Further, the framework (via the HCIS) also recognizes the multifaceted nature of the key participants within the healthcare system; in particular, the dynamics of their information requirements with respect to capturing, generating and disseminating of the necessary information. While our discussion focuses on the above three challenges impacting on the design and management of HCIS, the framework acknowledges the existence of other challenges. These challenges, though, are beyond the scope of this paper but are reflected in the framework for completeness. A key component of this framework is the protocols for ensuring HIPAA compliance, observing the principles of information integrity (I*I), and satisfying the healthcare quality aims (Q). Figure 2 depicts the proposed framework. Finally, the framework highlights the major deliverable from the HCIS; namely, the information product and its key applications to various healthcare practices and processes.

5.0 UK NHS ENVIRONMENT

In the UK, the National Health Service (NHS) is the "public face" of the publicly funded healthcare systems. The organisations provide the majority of healthcare in the UK (general practitioners, Accident and Emergency Departments, long-term healthcare and dentistry). Founded in 1948, they have become an integral part of British society, culture and everyday life. Private healthcare has continued in parallel to the NHS, largely paid for by private insurance, but still generally used by a small percentage of the population (and generally as a top-up to NHS services). NHS services are largely free at the point of delivery and are paid for by way of taxation. The NHS's budget for 2005-06 is over £80 billion and the Service employs over 1 million people and is ranked as one of the largest employers in the world. Healthcare in the UK has been the subject of global focus given the radical and far-reaching change programme currently taking place (NHS, 2006).

The lack of sufficient technological safeguards coupled with a lack of a comprehensive security vision and a policy statement on how to ensure healthcare information security are the major obstacles in way of the successful implementation and widespread uptake of the EPR concept. With the NHS, this viewpoint has been corroborated by the British Medical Association who have stated that currently "all the different parts of the NHS are not sufficiently encrypted and encoded up together" to ensure adequate information security to healthcare records (Crossley, 2002) . It is clear that there is existing technology that is in place and is sufficient to ensure that the EPR concept becomes a reality. However, the primary challenge continues to be the elusive hunt for a security mechanism that ensures the security of the information stored in EPR databases (Etheridge, 2001). The proposed integrative framework would be ideally suited to dealing with the new knowledge-based clinical era of the NHS.

6.0 CONCLUSION

In this maze of challenges currently facing healthcare, the need for well suited and high quality information that flows throughout the web of the healthcare system becomes paramount. HCIS can be used to most effectively and efficiently to facilitate the information flows and decision making throughout this healthcare system web. This should come as no surprise, given the general success of IS/IT in many business settings and the fact that healthcare is a data and information rich industry. However, what becomes a critical goal given the pivotal role for these HCIS then is to take a holistic and comprehensive approach to designing robust HCIS and subsequently effectively managing this asset. We have proposed an integrative framework as one approach to meeting this goal. Specifically, our framework considers the three key challenges of HIPAA compliance, the need for embracing the principles of I*I and the need to embrace the six healthcare quality aims. Moreover, the power of this framework lies in its universality since it is as suitable to the US healthcare environment which is essentially a private healthcare model as it is in the UK healthcare system which is dominated by a public model; namely the NHS.

7.0 REFERENCES

[1] American Institute of Medicine, 2001 Crossing the Quality Chasm – A New Health System for the 21st Century Committee on Quality of Health Care in America Institute of Medicine, National Academy Press, Washington, D.C.

[2] Health Insurance Portability and Accountability Act (HIPPA), 2001 Privacy Compliance Executive Summary, Protegrity Inc. May .

[3] Moore, T & R. Wesson 2002. "Issues regarding wireless patient monitoring within and outside the hospital" published in the 2nd Hospital of the Future Conference Proceedings, Chicago, USA.

[4] HIPAA Security requirement Matrix, 2002 - http://www.hipaa.org

[5] J. Perper 1994 "Life Threatening and Fatal Therapeutic Misadventures" in Human Error in Medicine, Bogner, M (Ed.), Lawrence Erlbaum associates, Publishers, Hillsdale, NJ. 27-52.

[6] Applegate, L., Mason, R. and Thorpe, D. "Design of a Management Support System for Hospital Strategic Planning", Journal of Medical Systems (10:1), 1986, pp. 79-94.

[7] Stegwee, R & T. Spil 2001. Strategies for Healthcare Information Systems, Idea Group Publishing, Hershey.

[8] Chandra, R., Knickrehm, M. and Miller, A. "Healthcare's IT Mistake", The McKinsey Quarterly (5) 1995.

[9] Geisler, E., D. Lewis, M. Nayar & P. Prabhaker, 2003 "Information Integrity and Organizational Performance: A Model and Research Directions" working paper

[10] Mandke, V M. Bariff and M. Nayar 2003 "Demand For Information Integrity In Healthcare Management" Forthcoming in The Hospital of the Future conference proceedings.

[11] Huang, K, Y. Lee, and R. Wang 1999. Quality Information and Knowledge Prentice Hall, New Jersey.

[12] Haag, S., M. Cummings and D. McCubbrey 2004. Management Information Systems for the Information Age 4th Edn. McGraw-Hill Irwin, Boston.

[13] Scott Morton, M. 1991. The Corporation of the 1990s New York, Oxford University Press.

[14] Thorne, K. and Smith, M. "Competitive advantage in world class organizations", Management Accounting (78:3) 2000, pp. 22-26.

[15] Wickramasinghe, N. and S. Sharma 2005 "Key Considerations for Ensuring High Quality HIPAA Compliant e-health" International J. Services and Standards (IJSS) vol 1 no. 3 pp. 319-335

[16] Wickramasinghe, N. in press "Patient Centric Healthcare Information Systems: The confluence of ethics, security and effective information systems" in Ed Quinnley, Encyclopaedia on Security and Ethics, Idea Group Hershey

[17] NHS 2006 Connecting for Health website. Available from: www.connectingforhealth.nhs.uk [Accessed 20 Sept 2006].

[18] Crossley, N. 2002. "Health: Access all areas: We all have the right to see our own medical records" The Guardian, pp. 2.16.

[19] Etheridge, Y. 2001. "PKI - how and why it works," Health Management Technology, vol. 22, Iss.1, pp. 20-21.