Ateneo Graduate School of Business

Our Country is *Our* Business!

Occasional Paper

No. 7

Assessing the Privacy and Security of Electronic Health Information in the Philippines: Informing the Philippine Compliance to the Expanded Trade of Healthcare Services in ASEAN

Eduardo P. Banzon

Juan Carlos A. Amores

Assessing the Privacy and Security of Electronic Health Information in the Philippines: Informing the Philippine Compliance to the Expanded Trade of Healthcare Services in ASEAN

Eduardo P. Banzon
Juan Carlos A. Amores

The Occasional Paper Series (OPS) is a regular publication of the Ateneo Graduate School of Business (AGSB) intended for the purpose of disseminating the views of its faculty that are considered to be of value to the discipline, practice and teaching of management and entrepreneurship. The OPS includes papers and analysis developed as part of a research project, think pieces and articles written for national and international conferences. The OPS provides a platform for faculty to contribute to the debate on current management issues that could lead to collaborative research, management innovation and improvements in business education.

Published by the Ateneo de Manila University
Graduate School of Business
Ateneo Professional Schools Building
Rockwell Drive, Rockwell Center, Makati City, Philippines 1200
Tel.: (632) 899-7691 to 96 or (632) 729-2001 to 2003
Fax: (632) 899-5548
Website: http://gsb.ateneo.edu/

Limited copies may be requested from the AGSB Research Unit
Telefax: (632) 898-5007
Email: submit@agsbresearch.org

Assessing the Privacy and Security of Electronic Health Information in the Philippines: Informing the Philippine Compliance to the Expanded Trade of Healthcare Services in ASEAN

Eduardo P. Banzon
Ateneo de Manila University
Graduate School of Business

Juan Carlos A. Amores
Ateneo de Manila University
Graduate School of Business

Abstract

The expanded use of electronic health records is expected to happen as ASEAN moves toward a single market for healthcare services. Experiences in other sectors, particularly the banking industry, show that as soon as the electronic exchange of information took off, the banking market opened up with freer flow of services. Faced with the same

situation, the healthcare sector must act now and adopt rules on the privacy and security of electronic health information. Not only would this address the need to maintain the physician-patient privilege, which has long been an established principle that governs health services information; but it would also help overcome persistent resistance of several stakeholders in healthcare to shift to electronically stored and transmitted health information. The resistance can be partly attributed to the fear that the electronic medium could compromise physician-patient privilege and that personally identifiable health information will be used against the physicians and the patients. This study hopes to address these concerns by determining the current regime on the privacy and security of electronic health information in the country and the measures that may improve this regime.

Keywords: policy, privacy and security of health information in the Philippines

Background

The member states of the Association of Southeast Asian Nations (ASEAN) have committed to a closer economic cooperation and collaboration during the Joint Statement of the 4th ASEAN+3 Health Ministers Meeting held in Singapore on 23 July 2012. This will be realized by increasing the flow of goods and services in various sectors and industries. The Roadmap for an ASEAN Community 2009 - 2015 (2009) identified the healthcare sector among the industries that it has pushed for an expansion of the flow and trade of good and services. In the last decade, ASEAN has slowly geared toward a freer flow of healthcare goods and services by slowly harmonizing the regulatory rules of drugs and cosmetics. To date, much progress has been achieved in cosmetics regulation than in drugs regulation. A limited mutual recognition agreement for nursing services was signed in 2006 but mutual recognition of home country nursing licenses has yet to happen. Nonetheless, despite the less-than-vigorous implementation of the commitments of the various ASEAN Member States to open up the trade of health goods and services, they will have to face the eventuality of a freer flow of healthcare trade among the countries in ASEAN.

According to the Philippine Overseas Employment Administration (POEA), in the last 10 years, Singapore has hired 2,200 Filipino nurses. The Philippines is also capable of providing health education services given that English is the medium of instruction in the country,

and it also has a vibrant private health education sector. The Philippines has increasingly been providing healthcare services to the other ASEAN member states, in or out of the country and on health education services.

As a member of ASEAN and a major provider of healthcare services, the Philippines has to prepare for the expansion of the trade of healthcare services. Several measures are needed to prepare the country, which include, but not limited to, the review of training and professional standards and the harmonization of the requirements for health professional licensing and practice. In this regard, a key area that needs to be evaluated is the country's regulatory and policy regime on the privacy and security of electronic health information.

As a member of ASEAN and a major provider of healthcare services, the Philippines has to prepare for the expansion of the trade of healthcare services.

The expanded use of electronic health records is expected to happen as ASEAN moves toward a single market for healthcare services. The obvious benefits from electronic exchange of health information in improving the quality and cost of healthcare imply that electronic health information would play a critical role in any ASEAN-wide expansion of trade in healthcare services. Experiences in other sectors, particularly the banking industry, show that once the electronic exchange of information took off, the banking market opened up with freer flow of services. The experience further shows that the adoption of rules on privacy and security of electronic banking information is critical in making online banking move forward.

The healthcare sector must adopt rules on the privacy and security of electronic health information to address the need to maintain the physician-patient privilege and also to overcome persistent resistance of several stakeholders in healthcare to shift to electronically stored and transmitted health information. The resistance can be partly attributed to the fear that electronic health information would compromise physician-patient privilege and that personally identifiable health information will be used against the physicians and the patients.

This study hopes to address these concerns by determining the current regime on the privacy and security of electronic health information in the country and the measures that may improve this regime.

Research Question

Given the ASEAN's call for expanded trade of healthcare services, does the Philippines have the laws, policies, guidelines, and private sector participation in ensuring the privacy and security of health information?

Methodology

The study will carry out a policy scan using the provisions of the Health Insurance Portability and Accountability Act (HIPAA), Health Information Privacy and Security Act (HIPSA), and Health Information Technology for Economic and Clinical Health Act (HITECH), as amended, of the United States (US). Two key informant interviews* will also be conducted to solicit information on Philippine laws that had specific provisions on the storage handling, and management of personal health information. The two respondents are medical doctors who have specialized in the use of information technology in the health care industry. The provisions of the US laws will be compared with current Philippine regulations and policies on health information and security. A review of related literature will also be conducted using the internet and grey literature search. For the research, the terms used included privacy, security, and standardization of health information.

* Personal Interviews with Dr. Ayedee Ace Domingo and Dr. Alison Perez

The US HIPAA and Related Laws

The US has evolved a healthcare system that is different from the social health insurance, national health system, or mixed models that most European countries have adopted. The US set up a government health insurance scheme for the elderly and the disabled, called the Medicare Program; and a government-subsidized health care for the poor managed at the subnational or state level, called the Medicaid Program. Those not covered by these programs are supposed to get their health insurance coverage through their employers. Unfortunately, this means that job loss or change may also result in the loss of one's current health insurance provider. Furthermore, the employment-linked health insurance coverage scheme increases the risks arising from the exchange of health information given that several players, including a large number of health insurance providers, are involved in providing and paying for healthcare services.

In 1996, the US enacted HIPAA to address the loss of or decreased health insurance coverage because of the pre-existing illness rule. The Act aims to ensure that Americans would have continuous health insurance coverage even if they move from one job to another (2007).

HIPAA included privacy rules to support the "administrative simplification" of electronic exchange of personal health information. The privacy rules included standards for the privacy of individually identifiable information or protected health information. The Act further provided rules on electronic healthcare transactions, medical privacy, security requirements, and enforcement

procedures. It laid down the guidelines for unique identifiers for employers, healthcare providers, and health plans.

The Act defined "protected health information" as "any information about health status, provision of healthcare, or payment for healthcare that can be linked to a specific individual." Health information was interpreted rather broadly; and it included any part of a patient's medical record or payment history.

HIPAA guidelines described the processes for individuals to access their personal health information in order to validate the correctness of the information while ensuring that the same information will not be accessed by unauthorized people.

The Act contained comprehensive provisions that spell out in detail the administrative safeguards, including security management process and workforce training and management, for protecting the sanctity of personal health information. In addition, it prescribed the rules on physical safeguards, including facility access and control and workstation and device security. Further, the Act stipulated the rules on electronic data interchange particularly health data dictionaries and the standard formats for electronically transmitted health information

HIPAA also established the standards for electronic signatures and the interventions that would facilitate inter-operability of health electronic systems, including the development and harmonization of privacy and security standards. It also proposed guidelines for the setting up of a Healthcare Information Technology Standards Panel and an Office of the National Coordinator for Health Information Technology.

In 2007, HIPAA was amended by the Health Information Privacy and Security Act or HIPSA, which expanded the protection of electronic health information by guaranteeing an individual's right to supplement, amend, correct, or destroy any of the individual's protected health information maintained or stored by an entity.

HIPSA created an Office of Health Information Privacy to oversee the implementation of the privacy provisions and to determine enhancements of existing rules. It created health literacy demonstration grants, which were expected to help people with low health literacy to exercise their privacy rights.

In 2009, HITECH was enacted to provide incentive payment to clinicians and hospitals for the use of electronic health records privately and securely. In addition to the incentives, HITECH strengthened the Office of the National Coordinator for Health Information Technology with expanded powers and resources, including the crafting of a strategic plan for a US-wide interoperable health information system.

HITECH extended the privacy and security regulations of HIPAA and HIPSA to information vendors and brokers, particularly when they partner with healthcare providers to create personal electronic health records.

The US has well established and extensive rules that define and safeguard the security and privacy of electronic health information.

Philippine Laws and Policies on Health Information

The Philippines does not have a specific law addressing security and privacy of electronic health information. The one law that discusses security and privacy of health information is the Philippine AIDS Prevention and Control Act of 1998 or the HIV AIDS Law. Although it is specific for information on HIV and AIDS, the law has provisions on the protection of electronic health information. The protected health information encompasses information that may include, but is not limited to, the name, address, picture, physical description, or any other characteristic of a person, which may lead to his/her identification as having undergone HIV testing or has been diagnosed to have HIV. The law mandates health professionals, health instructors, co-workers, employers, recruitment agencies, insurance companies, data encoders, and other health record custodians to protect health information.

The Philippines does not have a specific law addressing security and privacy of electronic health information.

However, the law provides exceptions to the privacy and security of health information by allowing waivers even without the consent of the individual. These exceptions include responding to subpoenas to testify in legal proceedings by those with access to the information. In addition, health workers who are exposed to invasive procedures and may potentially be in contact with blood and bodily fluids likely to transmit HIV shall be informed of the HIV status of a person, even without the consent of the patient. Furthermore, the law stipulates that the

following can be given the results of HIV testing: the parent of a minor who was tested; the legal guardian of an insane person or orphan who was tested; and a Judge of the Lower Court, Justice of the Court of Appeals, or Supreme Court Justice. Finally, any person with HIV is obliged to disclose his or her HIV status and health condition to his or her spouse or sexual partner at the earliest opportune time.

In addition to the HIV AIDS Law, the E-Commerce Act provides general guidelines for the privacy and security of all electronic information; hence, by extension, it includes electronic health information. Specifically, the E-Commerce Act provides protection of privacy and security for producers and users of electronic information. It explicitly allows individual choice and empowerment in determining the privacy and security tools to adopt; and it also mandates the private sector to make available to consumers the means to exercise choice with respect to privacy, confidentiality, content control, and even the anonymity of electronic information.

The role of government is to establish control processes and procedures as appropriate to ensure adequate integrity, security, and confidentiality of electronic data messages.

The law provides that parties to any electronic transaction shall be free to determine the type and level of privacy and security of electronic data message or document. They can select and use or implement appropriate technological methods that suit their needs.

The role of government is to establish control processes and procedures as appropriate to ensure adequate integrity, security, and confidentiality of electronic data messages, documents, records, or payments. The government is also mandated to ensure that any person who obtained access to any

electronic key; electronic data message; or electronic document, book, register, correspondence, and information shall not be allowed to convey to or share the same with any other person.

In order to implement the provisions of the E-Commerce Act, the government issued in 2009 Executive Order (EO) No. 810 which governs the application of digital signatures in e-government services. The EO aims to ensure the confidentiality, authenticity, integrity, and non-repudiation of electronic transactions in government. At the same time, EO 810 promotes the application of digital signatures in information technology systems in the private sector to ensure confidentiality, authenticity, integrity, and non-repudiation of electronic transactions in the sector.

Comparison

A wide range of rules and policies governing the privacy and security of electronic health information has evolved in the US in the last 15 years. The rules range from explicit definitions of protected health information to the creation of offices specifically tasked to ensure that the privacy and security provisions of the laws are properly implemented.

Table 1 shows the comparison of the US and the Philippine Rules and Policies on Privacy and Security of Electronic Health Information.

Table 1. Comparison of the US and the Philippine Rules and Policies on Privacy and Security of Electronic Health Information

Selected Rules and Policies on the Privacy and Security of Electronic Health Information	
US (HIPAA Privacy Rule, HIPSA, and HITECH)	**Philippines**
Privacy	
Definition of individually identifiable health information	Except for HIV-AIDS, none
Guidelines for access to protected health information	Except for HIV-AIDS, none
Harmonized privacy standards	E-Commerce Act provides limited guidance
Office of Health Information Privacy	None
Security	
Security standards for data storage and transfer	None
Rules on electronic signature	Present
Harmonized security standards	E-Commerce Act provides limited guidance
Other Provisions to Promote Inter-Operability of Electronic Health Information Systems	
Health data dictionaries mandated	Not mandated
National Coordinator for Health Information Technology	None
Monetary incentives for using electronic health records	None
Strategic plan for inter-operable health information systems	None
Grants to help people with limited access	None

The rules on privacy in the country provide adequate protection, but only to HIV-AIDS cases. The privacy provisions of the E-Commerce Act are also too general and do not specifically requires harmonizing privacy standards among all health stakeholders.

With regard to rules on security, a positive finding is the presence of rules governing electronic signatures in the Philippines that is similar to the rules in the US. However, there is limited guidance on security standards and the privacy provisions of the E-Commerce Act do not provide enough details for a sector-wide adoption.

As to other rules and policies to promote the inter-operability of health information systems of various private and public health stakeholders, there are no similar rules and policies in the Philippines as that in the US. There are no incentives for inter-operability; and there is no office or senior government official held accountable for promoting inter-operability or for the lack of such inter-operability.

The limited rules and policies governing privacy and security of electronic health information in the Philippines have resulted in the health sector evolving its own responses to the need for privacy and security.

The limited rules and policies governing privacy and security of electronic health information in the Philippines have resulted in the health sector evolving its own responses to the need for privacy and security. Hospitals and other healthcare organizations have developed their own policies, processes, and systems to ensure the protection of patient-related information. As a result, systems developed are fragmented, which do not contribute to inter-operability and expanded use of electronic health information. This issue is

compounded by the lack of incentives or strategic plans to promote the inter-operability of systems developed by healthcare institutions.

The fragmentation of interventions for privacy and security of electronic health information also means that health providers will not be able to access the necessary health information when needed. This situation makes the aggregation of health data from both public and private sectors difficult, resulting in a general lack of aggregated health information in the country.

The fragmentation of interventions for privacy and security of electronic health information also means that health providers will not be able to access the necessary health information when needed.

Recommendations

There are significant gaps in rules and policies governing privacy and security of health information in the Philippines. The limited rules and policies that now exist explicitly include the private sector in maintaining privacy and security; but the lack of comprehensive policies has resulted in uncoordinated private sector initiatives. This situation has led to fragmented electronic health information system in the country. The comparison of HIPAA and related laws of the US with existing Philippine laws clearly shows that there is a wide opportunity to craft a comprehensive law that would include, but not limited to, the following:

1. definition of protected health information,
2. description of privacy and security standards,
3. creation of offices responsible for promoting the privacy and security of health information,
4. incentives for developing the inter-operability of electronic health information systems and for assisting low health-literate persons, and
5. crafting of national strategic health information plan.

In pursuit of the universal healthcare reform agenda of the Aquino administration, the promulgation of a comprehensive health information law that promotes security and privacy becomes imperative. With the expected integration of health services in ASEAN, a comprehensive law would enable the Philippines to adequately prepare for integration. With the extensive experience of the US in evolving its laws and policies on secured health information, using HIPAA Privacy Rule, HIPSA, and HITECH as templates for the proposed Philippine law may be a rational step forward.

References

ASEAN. (2009). Roadmap for an ASEAN Community 2009–2015. Retrieved fromhttp://www.aseansec.org/publications/RoadmapASEANCommunity.pdf

Barrows, R. C., Jr., & Clayton, P.D. (1996). Privacy, confidentiality and electronic medical records. *Journal of the American Medical Informatics Association, 3*(2), 139–148.

Blumenthal, D., & Tavenner, M. (2010). The "meaningful use" regulation for electronic health records. *New England Journal of Medicine, 363*(6), 501–504.

Blumenthal, D. (2009). Stimulating the adoption of health information technology. *New England Journal of Medicine, 360*(15), 1477–1479.

Center for International and Strategic Studies. (2010). ASEAN Roadmap for Integration of the Healthcare Sector. Retrieved from http://pdf.usaid.gov/pdf_docs/PNADJ869.pdf

Executive Order No. 810, S. 2009. Retrieved from http://www.gov.ph/06/15/excutive -order-no-810-s-2009/

James, D. G. (2007). HIPAA in healthcare: Information security in a healthcare environment. Retrieved from http://www.infosecwriters.com/text_resources/pdf/InfoSec_In_Health_Care_DJames.pdf

Philippine AIDS Prevention and Control Act of 1998 (Republic Act No. 8504). Retrieved from http://www.chr.up.ac.za/undp/other/docs/legislation3.pdf

The E-commerce law (Republic Act No. 8792). Retrieved from http://www.pctc.gov.ph/initiatv/RA8792.htm

Summary of HIPAA Privacy Rule. Retrieved from United States Department of Health and Human Services website: http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/index.html

Summary of HIPAA Security Rule. Retrieved from United States Department of Health and Human Services website: http://www.hhs.gov/ocr/privacy/hipaa/understanding/srsummary.html

Health Information Privacy and Security Act of 2007, S. 1814, 110th Cong. (2007). Retrieved from http://www.govtrack.us/congress/bills/110/s1814/text

Philippine Overseas Employment Administration Employment Data. Accessed on August 8, 2011 from http://www.poea.gov.ph

Dr. Eduardo P. Banzon is the president and chief executive officer of the Philippine Health Insurance Corporation (PhilHealth). Prior to this post, he was a senior health specialist at the World Bank. And before he joined the World Bank, he was PhilHealth's vice president of the Health Finance Policy Sector: Dr. Banzon graduated from the University of the Philippines, College of Medicine, with a degree of Doctor of Medicine. He obtained his Master of Science degree in Health Policy, Planning and Financing from the London School of Economics and the London School of Hygiene and Tropical Medicine. Dr. Banzon is a faculty member of the Health Unit of the Ateneo Graduate School of Business, where he teaches in Master of Business Administration (Health) program. He was a clinical associate professor at the University of the Philippines, College of Medicine, where he taught health economics, health policy studies, and community medicine, in both the medicine and post-graduate degree programs. As a research associate professor of the National Institute of Health, he focused on health screening interventions. He also served as a community health physician at the Philippine Rural Reconstruction Movement and the International Institute of Rural Reconstruction.

Juan Carlos A. Amores is an information technology (IT) consultant specializing in web design and project management. He has been an IT consultant at the Ateneo Graduate School of Business on project management, training, and research in its Health Unit.

He is a project associate at the Health Unit, responsible for designing and implementing IT-related activities in line with the expansion of the unit. Before this engagement, Mr. Amores was project data specialist and field research supervisor for the 2011 Assessment of Mass Media-Based Health Communication Campaigns of the Department of Health (DOH), which was undertaken by the Health Unit. His initial involvement with the Health Unit was as documentor for the Management for District Health Systems Training Course sponsored by InWent, Germany.

He graduated from the Ateneo de Manila University in 2009 with a Bachelor of Science in Management Information Systems. He is one of the incorporators of Zeaple, a web development and IT consulting company offering a variety of IT solutions in the areas of website development, content management system, mobile application, data mining, custom application, and systems development.