Negotiating privacy, confidentiality and security issues pertaining to electronic medical records in Sri Lanka: A comparative legal analysis

Harshani Menaka Ratnayake Attorney-at-Law, Masters in Information Technology, Banking and Labour Law (L.L.M), Post-Attorney Advance Dip. in Banking, Finance and Insurance Law
E-mail address: menakaratnayake@yahoo.com

Sri Lanka Journal of Bio-Medical Informatics 2013;**4**(2):32-39
doi: http://dx.doi.org/10.4038/sljbmi.v4i2.5859

Abstract

Introduction
Sri Lanka is set to adapt electronic medical records (EMR) at an ever increasing rate in the coming decade. However, handling of EMRs pose considerable legal challenge in relation to its privacy and confidentiality, quality of records and tort based liability. While the Sri Lankan legislation recognise electronic records as legally valid in most instances, it does not provide sufficient legal backing when it comes to sensitive personal health data.

Methodology
This paper adapts a comparative method of legal research. The author believes this to be an appropriate methodology for answering the research questions as it is primarily used for the purpose of "promotion of mutual understanding by acquiring knowledge of foreign legal systems".

Findings
The paper recognizes that the existing Sri Lankan legislation does not provide for sensitive personal data such as EMR. However, the Sri Lankan legislation has already established the legal validity of electronic records. The paper discusses various legislations from the US including the Health Insurance Portability and Accountability Act (HIPAA) of 1996, The Patient Safety and Quality Improvement Act (PSQIA) of 2005 and Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009 as reference legislation. It also discusses the Data Protection Act of 1998 in the UK and the EU Directives as reference legislation for establishing a legal framework for Sri Lanka that would address the needs of EMRs.

Recommendations
Following the legal analysis, the paper proposes a way forward in adapting suitable legislations from the ones discussed. Some of these adaptations include defining the criteria in which a valid legal record can be established, the creation of the role data controller, laying down a clear framework in which personal health data can be shared, defining the criteria that should be met when using EMR for research, measures to encourage the adaption of EMRs and the standards set forth and the necessity to amend the Computer Crimes Act to include specific provisions to deal with crimes involving EMRs.

Conclusion
The paper concludes by stating the need to obtain wider consensus from all relevant stakeholders before such legislation is implemented and that the same should not hinder the IT industry which can promote the efficiency of the country's health care system.

Keywords - Electronic Medical Records, data protection law, privacy, comparative legal research

Introduction

In modern day medical practice, clinicians as well as health managers rely more on health information than ever before. The inability to make use of paper based health records in emergency care management and in continued care of patients have made health professionals and managers frustrated and grappling for solutions. Computerising personal health data is probably the most obvious answer to many of these challenges[1,2,3].

Although slow and backward in its incorporation, Sri Lanka has seen a surge in incorporating technology into the medical field, especially in relation to storing and managing medical data. Thus Electronic Medical Records (EMR) is no longer a strange term for the Sri Lankan health community. However, EMRs also have its downsides. Among them, security and privacy issues related to health data have become widely debated issues and it may be particularly serious in a country such as Sri Lanka where evolution of technology does not go hand in hand with the evolution of other associated fields such as the necessary legal frameworks.

In this backdrop, this paper examine the legal pitfalls that would arise as a result of implementing EMRs, present legal backing in relation to patient records in Sri Lanka, the legal provisions existing in other parts of the world in order to tackle such issues and the necessary adaptations to be made to the related legal framework in Sri Lanka.

Methodology and the structure of the paper

This paper will adapt a comparative method of legal research[4]. Thus, the author will be focusing on the legal family known as the 'common law family' which includes the legal systems of England and USA with other legal systems being approached as necessary. The paper will first analyse the available literature in order to enumerate the legal challenges emerging from the use of EMRs. The paper will then discuss the available legal provisions in Sri Lanka and in the rest of the world with regard to dealing with the recognised legal challenges and will suggest necessary amendments in order to strengthen the legal framework to safeguard patient rights as well as not to stall desirable industry progression.

Legal concerns in relation to EMRs

According to the available literature, the commonest forms of legal challenges emanating directly from the use of electronic medical records can be recognised as,

a. Privacy of patient information.
b. Reliability and quality of records and,
c. Tort based liability[5].

However, as pointed out by Hodge[6], these three concerns are inherently interconnected and therefore the policymakers should be aware about the implications of their actions on all areas concerned.

a. Privacy of patient information

Patient's privacy refers to the right of a patient to expect that their health information remains private and shared with others to the extent in order to provide proper health care. While admitting that there is no definite meaning to information privacy, Nass[5] points out that it [privacy] could mean different things to different people. Privacy would take its perceived form depending on the context, based on the 'stated reasons for the information being gathered, the intentions of the parties involved, as well as the politics, convention and cultural expectations'[8]

As health information systems proliferate, so does the number of users engaged in handling personally sensitive data[9,10]. While having immediate access to personal information for providing patient care is immensely useful in the clinical management of a particular patient,

the danger is that many other individuals might also access the same information for secondary and sometimes unwarranted uses[11].

b. Reliability and quality of records

In the process of feeding information to EMRs, 'short-cuts' taken by the physicians as well as by other health staff could lead to a substantial loss of data quality and accuracy[12]. Furthermore, when physicians are more worried about updating the computer record than doing a proper assessment of the patient concerned, room for malpractice is inevitable[13]. In some instances, patient related data will be entered into the system by a nurse or a data entry operator. When this is un-supervised, the quality and the accuracy of the data being entered into the system are highly questionable[13].

c. Tort based liability

Liability issues arising in relation to EMRs can be attributed to breeches in privacy and confidentiality as well as to the poor quality and reliability of medical records as discussed earlier[14,15]. Such liability may arise in relation to disclosure of information through email, internet or through computer networks[6]. However, unless proper regulatory mechanisms are in place to trail such disclosures, it becomes nearly impossible for the law to function and for such claims to move forward.

Present legal framework governing EMRs in Sri Lanka

According to the World Health Organisation (WHO) GOe survey, manual medical records in Sri Lanka is considered a legal document and only authorized personnel can access such records[16]. In an article published in the Daily News titled 'Law on Information and Communication Technology', Mr Sunil Abeyratne (Attorney-at-Law) states that, "As far as the present legal provisions are concerned, Sri Lanka is not second to any other developed or developing country in dealing with ICT related matters subject to few exception"[17]. With the enactment of the Electronic Transactions Act No. 19 of 2006, the electronic records and communications received legal validity and therefore electronic medical records which are created in an acceptable manner should receive the same legal status as their paper forms. The Computer Crime Act No. 24 of 2007 is also useful in dealing with EMRs as it provides for "criminal implication regarding unauthorised access to a computer, computer programme, data or information and unauthorised use of a computer"[18].

Laws governing EMR practices in the developed world

US legislations

The Health Insurance Portability and Accountability Act (HIPAA) of 1996 identify certain guidelines as to how health information should be shared[19]. The Act recognises several 'covered entities' such as insurance companies, health care clearing houses, employer sponsored health care plans, and certain medical service providers. Accordingly, 'covered entities' should disclose the patient information to the patients on request within a stipulated time period and thus nullifies the possibility for 'information withhold'. Secondly, the Act defines the provisions for disclosure to a third party and these instances include facilitating treatment, payment, health care operations, requested by law or requested with the consent of the patient concerned. Another section of the HIPAA directly deals with EMRs and it

enforces the need to have security safeguards to comply with the Act. Accordingly, an entity should disclose the administrative procedures and policies in handling such EMRs, they should implement procedures to prevent unauthorised physical access to patient records and should also adhere to sound safety practices when transmitting data through a network to prevent any unauthorised access.

In 2013, HIPAA was further enhanced by adding the final omnibus rule, which was aimed at strengthening patient privacy and information security in a continuously evolving digital age[20]. Thus, HIPAA now recognises that the business associates are not only responsible for their own compliance with the rules preventing data breeches but they should also be responsible for the compliance of their sub-contractors even when the subcontractors do not use or handle such data.

Until the Final Omnibus Rule took effect in 2013, it was the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009 which made interim changes to HIPAA. However, one of the main focuses of the Act was to enhance the uptake of EMRs through the provision of performance incentives and funds to adapt for practitioners and healthcare institutions. It was a strategy to accelerate the use of EMRs in the US. The importance of the Patient Safety and Quality Improvement Act (PSQIA) is the legal covering it gives to 'patient safety work products' which includes data analyses, memoranda, reports, and records that may affect the outcome of treatment or improve patient safety[21].

Apart from the above, the American Recovery and Reinvestment Act of 2009 addresses unauthorised sale of medical records. It emphasises that such actions can be warranted in instances such as research, public health and treatment[22].

UK legislation

The Data Protection Act of 1998 deals with sensitive information such as health records in a separate section while recognising the need to communicate such information between professionals. It further derives the necessity for the patient to know who will share their data and for what purpose. An important aspect of this legislation is the defining of eight principles in which personal data such as EMRs become legally acceptable. Thus, in order to be accepted as legally valid, information should be:

- fairly and lawfully processed,
- processed for limited purposes,
- adequate, relevant and not excessive,
- accurate,
- not kept for longer than is necessary,
- processed in line with subjects' rights,
- secure,
- not transferred to countries without adequate protection[23],

At the same time, the Electronic Communications Act of 2000 allows the creation and transmission of prescriptions while putting down certain conditions to fulfill its validity [23]. An important element in the UK legislations related to data protection is the establishment of a data commissioner[24]. Thus, non-governmental organisations including medical practitioners should register themselves as personal data handlers and should file a notice with the data commissioner regarding the type of personal data being handled, why it is

processed, persons to whom the data will be sent, etc.

In recent times, there has been a move to strengthen the data protection directives of the European Union, which would in turn affect the regulations governing personal medical records in the UK. In this regard, the British Medical Association (BMA) emphasises the need to strengthen the individual's right and enhance the internal market dimensions through such amendments while adhering to the basic principles of the UK Data protection Act. In that, the BMA suggest allowing the data controllers to apply a risk-based process of determining personal data by considering the context to which the data belongs[25]. Furthermore, pointing out the fact that sensitivity of personal health data would vary from person to person or from one location to another, the BMA also emphasies the need to take a contextual approach towards handling personal health data.

Adopting to the emerging challenge: The way forward

While acknowledging the fact that the Sri Lanka Electronic Transaction Act provides for electronic records to be recognised as legally valid, it may well be justified to evaluate and adapt some of the principles that determines a 'legal' record in the UK Data Protection Act to address the sensitive nature of EMRs. At the same time, defining the security requirements at each level of design, implementation and operation of such EMR solutions, such as in the case of HIPAA, should also be a matter for discussion when formulating such legislation. In addition, a country such as Sri Lanka could well nurture a data controller, as in the UK and other EU countries, that has the power to authorise or object to handling of personal health data, and if non-compliant to take legal action against those who wilfully breech the trust placed on such entities.

Another aspect that the Sri Lankan Laws should be clear about is the sharing of personal health data for the benefit of the patient, in order to uplift public health status and for better resource distribution. In doing so, Sri Lanka can implement a framework to recognise 'responsible entities' with regard to handling personal health data as in the case of HIPAA. The framework should establish the need to maintain audit trails of personal health information flow and to be transparent in all such acts of information sharing.

While it is desirable that informed consent from the patient be made mandatory for personal health data sharing, stakeholders should decide the instances in which obtaining such consent can be waivered in order to perform emergency care procedures, undertake rapid responses to public safety hazards, etc. Furthermore, as pointed out by the BMA, handling and sharing of genetic information should also be recognised as a data set needing special attention and specific regulations.

As was the case with the HITECH Act of 2009, it may also be useful to encourage the medical organisations and individuals to undertake EMRs for their practices although given the lack of basic infrastructure and the presence of a sound legal backbone, such encouragement should be done with caution. However, standardising such technology uptakes may help the implementation of the laws better than when there is an EMR industry which lacks standards and are haphazardly adapted to facilitate individual needs of healthcare organisations and practitioners.

Conclusion

The present legal framework governing EMRs in Sri Lanka can be considered weak in the context of rapid adaption of electronic means for patient records and its transmission. This may negatively affect the future of the health status in Sri Lanka. Therefore, it is high time to convene all the stakeholders including patient groups for discussions on enacting the government policy in relation to EMRs and towards e-Health as a whole.

References

1. Hillestad R, Bigelow J, Bower A, Girosi F, Meili R, Scoville R et al, Can electronic medical record systems transform health care? Potential health benefits, savings, and costs. Health Affairs 2005; **24**(5): 1103-17.
http://dx.doi.org/10.1377/hlthaff.24.5.1103

2. World Health Organization. Medical record manual: a guide for developing countries (Western Pacific Region). WHO; 2006. p. 4.

3. RAND. Health Information Technology: Can HIT Lower Costs and Improve Quality? Health Division. 2005.
Available at:
http://www.rand.org/content/dam/rand/pubs/research_briefs/2005/RAND_RB9136.pdf.
Accessed on: 5/6/2013.

4. Church J., Edwards AB. Comparative law/Comparative method. Hosten et al. Introduction to South African Law and Legal Theory. Butterworths. 1995; 1261-70.

5. Nass SJ, Laura AL, Gostin LO. Eds. Beyond the HIPAA Privacy Rule: Enhancing privacy, improving health through research. National Academies Press, 2009.

6. Hodge Jr JG, Gostin LO, Jacobson PD. Legal Issues Concerning Electronic Health Information: Privacy, Quality, and Liability. The Journal of the American Medical Association 1999; **282**(15):1466-71.
doi: http://dx.doi.org/10.1001/jama.282.15.1466

7. Saha S. Electronic medical records – European perspective. Industry Analysis for Frost & Sullivan. April 2004.
Available at: http://www.frost.com/prod/servlet/market-insight-top.pag?docid= 17055864.
Accessed on: 4/9/ 2012.

8. Nissenbaum H. Privacy as Contextual Integrity. Washington Law Review. 2004; 79:101-39.

9. Win KT, Willy S, Yi M. Personal health record systems and their security protection. Journal of Medical Systems. 2006; **30**(4): 309-15.
doi: http://dx.doi.org/10.1007/s10916-006-9019-y

10. Gostin L. Health Care Information and the Protection of Personal Privacy: Ethical and Legal Considerations. Annals of Internal Medicine. 1997; 127(8): 683-690.

doi: http://dx.doi.org/10.7326/0003-4819-127-8_Part_2-199710151-00050

11. Institute of Medicine Committee on Improving the Patient Record. In: Dick RS, Steen EB, eds. The Computer-Based Record: An Essential Technology for Health Care. Washington, DC: National Academy Press; 1991.

12. Hartzband P., Groopman J, Off the record--avoiding the pitfalls of going electronic. New England Journal of Medicine 2008; 1656-8.
http://dx.doi.org/10.1056/NEJMp0802221

13. Korin J., Quattrone M. Electronic health records raise new risks of malpractice liability. Law.com. 2007.
Available at :
http://www.law.com/jsp/legaltechnology/pubArticleLT.jsp?id=1182194746807.
Accessed on: 17/2012.

14. Vickery AB. Breach of confidence: an emerging tort. Columbia Law Review 1982; **82**:1426-68.
doi: http://dx.doi.org/10.2307/1122268

15. Zelin JE. Annotation, physician's tort liability for unauthorized disclosure of confidential information about patient. American Law Report.1988; **48**:668

16. Rampitige R. Global Observatory for eHealth (GOe) Survey in Sri Lanka. Sri Lanka Journal of Biomedical Informatics 2010; **1**(1): 49-52.

17. Abeyratne SDB. Law on information and communication technology. Daily News. 24 March 2011.

18. ICTA, e-Laws project.
Available at: http://www.icta.lk/index.php/en/e-laws-project#LEG.
Accessed on: 19/3/2013.

19. US Department of Health and Human Services, Health information privacy.
Available at: http://www.hhs.gov/ocr/privacy/hipaa/understanding/index.html.
Accessed on 20/3/2013.

20. U.S Department of Health and Human Services. New rule protects patient privacy, secures health information. News release. HHS press office. January 17th 2013.
Available at: http://www.hhs.gov/news/press/2013pres/01/20130117b.html.
Accessed on 1/3/2013.

21. Rockville MD. The Patient Safety and Quality Improvement Act of 2005. Overview. Agency for Healthcare Research and Quality.
Available at: http://www.ahrq.gov/qual/psoact.htm.
Accessed on: 19/4/ 2013.

22. Electronic Privacy Information Center. American Recovery Act Includes Strong Medical Information Safeguards. News Bulletin.
Available at http://epic.org/privacy/medical/

Accessed on: 23/6/2013.

23. Royal College of General Practitioners. Good practice guidelines for general practice electronic patient records (version 3.1). Department of Health. June 2005. Available at: http://www.connectingforhealth.nhs.uk/systemsandservices/infogov/igsoc/good-practice.pdf. Accessed on: 5/6/2013.

24. Donald CD. International Data Protection and Privacy Law. Practicing Law Institute. 2009.

25. British Medical Association. A comprehensive approach on personal data protection in the European Union, BM response. EU consultation. 2010/2011. Available at: http://ec.europa.eu/justice/news/consulting_public/news_consulting_0006_en.htm. Accessed on: 10/6/2013.