23 September 2006

Dear SMA Member,

MEDICAL RECORDS IN WEB-BASED SYSTEMS

We have received queries from members about the management and storage of medical records in web-based systems, and in particular, the liabilities of the PHMC-registered clinic and doctor.

We have consulted our Honorary Legal Advisors, and forward for your attention, the legal opinion from one of our Advisors. We urge you to read especially paragraphs 6 and 7 very carefully.

Additionally, another of our Advisors is of the opinion that at least one of the companies has unacceptably broad disclaimers of warranties and limitation of liability clauses, which seek to avoid liability for matters which are under its control.

We hope you will find the information useful.

---

1. The Private Hospitals and Medical Clinics Act does not make it unlawful per se for hospitals to consider using a web-based CMS to manage, store and retrieve confidential patient information, so long as the hospitals continue to keep and maintain the primary records on their own, which is required by the Private Hospitals and Medical Clinics Regulations (2002 Revised Edition) Section 12.

QUESTION:

What are the liabilities of the HCI and the doctor if medical records are data-mined without the explicit consent of the doctor or patient?

2. The issue relates to whether explicit consent is necessary. I am of the view that the fact that HCIs may

need to engage outside vendors and specialists to help them manage medical records in a digital format, is also not in itself new or novel and there is a reasonable argument in favour of attributing some degree of implied consent to the possible involvement of such third parties, who may have access to confidential patient information in the course of the services they provide. This is of course, subject to the proviso that the HCIs make every effort to ensure that these third parties agree to be bound by a duty of confidentiality. HCIs should also seek the third party's contractual indemnity to cover them for potential liability in the event the obligations are breached.

QUESTION:

What are the liabilities of the HCI and the doctor if the IT company ceases operations temporarily or permanently for any reason, and business continuity is compromised? What are the liabilities of the HCI and the doctor if data is illegally accessed or compromised (e.g. hacked)?

3. The issue is whether the legal position is now different because the data is to be on an off-site location and more importantly, it is effectively provided to a third party to manage, maintain and control, albeit within the confines of the contractual terms of engagement set by the HCIs. Would this then require that explicit consent be sought from the patients? I am of the view that if we accept that within the Singapore healthcare system, the need to use outside vendors and agents to manage medical databases may conceivably be said to be within public knowledge, then the argument of implied consent would be a strong one, whether or not it is a web-based CMS or something more limited in scope. The question is, is it reasonable to say that it is within public knowledge? The argument is probably about as strong as saying that we have arrived at a stage where the ability of the EMRX to allow cross-HCI access to medical information is now a fact within the public domain. I am just not sure that we are at such a stage yet, although this is certainly now more widely known than when EMRX was first launched.

4. Therefore I would venture to say that our ability to defend any claim or allegation that there has been a breach of confidentiality with the use of a web-based CMS may not be as strong or assured as I would like to have before going into such a project. I would say that the argument of implied consent for web-based CMS involving an external party is probably weaker than for cross-HCI access to EMRX. However I would add that this is often the case when something is newly introduced. When the Courts introduced the Electonic Filing System it did entail the engagement of a third party IT company to manage and handle confidential court papers and one could have similarly said that there could be confidentiality concerns.

5. I should add that usually no one complains when the system is working efficiently and effectively but complaints usually arise when there is a problem. The fact that you are entrusting a third party over whom you have no direct control does mean that the HCI is at the mercy of the IT company if the IT company should go into financial difficulty, has personnel issues or technical problems that affects its ability to provide the services as needed. This can occur, as you said, if there is any disruption to services, or in the case of hacking. Furthermore, if despite the contractual obligation of confidentiality, the company's staff misuses the information the HCI is still directly answerable to the patient, who may at this stage argue that his or her consent was not sought before the third party was allowed to handle the confidential records and he or she objects to it.

QUESTION:

Is explicit patient consent required when the HCI uses a web-based CMS and the HCI is therefore not custodian of the patient's data?

6. Whatever the case, even if the patient accepts that the HCI may need to and has engaged the services of an IT company to provide web-based CMS, I am of the view that in the event of any disruption, compromise or breach in the system that may affect delivery of care or even if it is simply a confidentiality issue, ultimately the HCI still remains responsible to the patient. The HCI is unlikely to succeed in any attempts to wash their hands of the matter and simply to redirect the claims to the IT company with whom the patients have no direct relationship. The HCI's protection comes in the form of contractual indemnities that it may seek from the IT company, and it must still be concerned as to whether these companies are financially sound companies who are able to fulfil their obligations. However if you look at the sample contracts you provided, you will see that on the contrary IT companies may seek indemnities from the HCI and may further impose various limitations or disclaimers in liability to protect themselves. They may also make it clear that they will not be responsible for any claims from patients and it is the HCIs' problem to deal with these. Therefore HCIs must be well aware that the contractual terms of engagement with these companies may leave them at the mercy of the IT company's effectiveness, reliability and security, not to mention the integrity of the personnel handling the information, and it is something they must be prepared to answer for in the event problems occur.

7. HCIs who wish to go ahead with web-based CMS will do well to manage their risks by (1) at least highlighting this to the patients in the general information relating to the hospital services that are provided to the patients, if not seeking explicit consent; (2) ensure that they deal with reputable and financial sound IT companies who are reliable and have good security systems as well as backup systems to ensure continuity of access and (3) ensure that the indemnity provisions and limitation of liabilities are not drawn up on terms that are totally unfavourable to them. My own sense is that the use of such a system may quickly become well accepted, in which case the concerns regarding confidentiality may start to lessen over time.

PREPARED BY:

MS KUAH BOON THENG
LEGAL CLINIC LLC
