Security of Practice Management Systems in General Practice.

Table of Contents

Introduction:

With the ever-increasing use of ICT in our medical practices and the increasing consciousness of our patients' rights to privacy and confidentiality, it is incumbent on us as Health Care Practitioners (HCP) to be cognisant that the technologies we implement in our work places are fit for purpose.

New Zealand legislation exists to protect the privacy of individuals and information about individuals(Privacy Commisioner, 1994, Health and Disability Commisioner New Zealand, 1996, 1993). The legislation also provides the basis upon which our professional organisations make recommendations around best practice and expected ethical standards(RNZCGP, 2011, NZMA, 2011, Medical Council of New Zealand, 2001). Our patients expect to have their secrets and confidences protected at the highest levels available.

That confidence, to protect client information, has been shaken of late by such public failures as has occurred with the ACC, IRD and EQDC. There would be few, if any, HCP who at sometime in their practicing careers have not been in breech of their legal and/or ethical obligations to their patients' confidences, whether that be of a minor or serious nature.

It is the purpose of this paper to investigate the most widely used Practice Management Systems (PMS) in New Zealand general practice and to ascertain the functionality of each PMS to keep the patient's Health Care Record secure.

Literature Review:

Since 2000, NZ General Practice has achieved 100% Electronic Health Record (EHR) uptake and is only second to Denmark in the use of EHR across the Health System(Jacobs S, 2011). This is a reflection on New Zealander's enthusiasm and ability to use advanced technologies for their ongoing benefit. With this in mind however there is still some reticence held by the New Zealand public as indicated in focus groups convened by the IT HealthBoard when discussing security and privacy issues around the EHR. (IT HealthBoard, 2011). This is a reflection of what has been documented in the literature to date(Cushman et al., 2010). New Zealand's recent breaches of privacy, e.g. ACC, Ministry of Social Development and Ministry of Justice, will have heightened the public's awareness and acuity around the potential harm that may arise out of the unintended release of personal information into the public arena. That being said the advantages of the EHR can be seen by the public as long as the concerns around security, confidentiality and access are addressed(Ryan K M, 2004).

Our financial and legal colleagues have already sought to address these issues as they pertain to their particular professions. Security of the patient's EHR is seen as a potential risk but the public wanted to know that these were being minimised and we are paying attention to mitigating this risk(Ryan K M, 2004). One would expect confidence to grow around their EHR just as it has in their acceptance of online and mobile banking(Klein C,

2011). The patient wants to know explicitly how those collecting their personal health information were having this addressed.

Patients expect an increasing depth of expertise in their healthcare so too should the HCP provide an increasing depth and breadth of security around the EHR. The increasing complexity around the provision of technology is outpacing the ability of the HCP to maintain the security and privacy requirements of the EHR. It is necessary to understand ones own limitations and seek appropriate help and advice with respect to any technology(Mohan P, 2011). We will need to develop relationships with qualified Health Informatics Professionals (HIP) who are duly accredited and certified. These HIPs will understand the special obligations they have with the delivery of the EHR. This will release the HCP to concentrate their attention on healthcare not computer care.

To mitigate our security risks associated with EHR we need to understand whether our administrative, physical and technical standards are addressed. Does the PMS we use adequately address those areas of potential risk and how are these potential risks mitigated? Are our providers adequately certified and compliant? "While breaches of compliance may occur, ensuring privacy in the digital era appear to be more error proof than… in the paper record." Breaches of confidential information has more to do with human error than it does with IT shortcomings(Matasar-Padilla, 2012).

We need to be sure that any shared data is de-identified to an internationally accepted standard. In the US this is stipulated by HIPAA where eighteen specific identifiers need to be removed before it is used for population health benefits(Klein C, 2011). We know that 87% of the US population can be uniquely identified simply form their birth-date, gender and zip code(Zetter Kim, 2009). Shared data is that which is legally required or consented to by the patient. However we learn that the use of de-identified data is accepted as an "altruistic" side of everyone(Ryan K M, 2004).

Method:

Each of the three main suppliers of Practice Management Systems available in New Zealand was surveyed. They were asked questions about the built-in security features

as set out by ISO/IEC27002, ISO 27799 and IEC 61508 as has been adopted by those implementing EHR(Dr Laurence Knott, 2012)(see appendix 1). These vendors included Medtech Ltd (PC), Houston Medical (PC), and IntraHealth-Profile for Windows (PC) and Profile for Mac (Apple).

The questions were arranged in order to identify the security that each had in place around four main headings.

1. Access Control.
2. Orders and Recording.
3. Audit and Logging.
4. Backup and Validation.

Results:

Access Control:

Though the vendors supplying the PMS that responded indicated that they had a means of authentication there was no mandatory minimum length or character set. Profile would write a macro on request but this had to be requested by the practitioner. There was no mandatory forced change of passwords, though again Profile was able to have this implemented in a security option.
Both Houston and Profile have the ability to assign different levels of access through role authorization.
There was some form of time out feature available within the settings of the PMS.
Both Houston and Profile had encryption protocols and Profile has implemented AES 256 encryption between its clients and server.

Orders and recording:

Both systems had tracking of orders and complied with HL7 protocols. They both provided pre-coded data choice selections to reduce error.

Audit and Logging:

All complied with audit and logging standards.

Backup:

Profile had an automated backup procedure that could be scheduled but Houston did not. Profile had only a few data validation functions whereas Houston did this on a regular basis.

Other Comments:

Intrahealth is ISO certified under ISO13485 and also implements IEC standards where appropriate. (ISO13485 is usually harmonized with ISO9001). Our web portals and IOS devices meet the industry standards on encryption (SSL 128-bit etc.)(Ross Montgomery, 2013).

MOH and ACC are accreditiors(Gin Gray, 2013) for Houston Medical.

At the time of writing Medtech Global had yet to reply to the questionnaire.

Discussion:

We know there is an international Information Security Standard, the ISO27000-ISO27009. The equivalent New Zealand Standard is the AS/NZS ISO/IEC 27000:2006. Of particular interest in this project was how well our commonly used PMS comply with these standards.

It is apparent that there is no incentive for the common PMS in New Zealand, that I surveyed, to meet these standards. The implementation of the EHR in New Zealand and in particular general practice has been a decision made by the principals who control and own these private businesses. There have been no regulatory controls enforcing the

meeting of these international standards. This would appear to be a voluntary requirement. World Health Organisations view New Zealand General Practices as world leaders in the implementation of the Electronic Patient Record (EPR). In fact 100% of general practices have an EPR of some iteration.

Since the first introduction of EPR in the late 70's early 80's it was thought that just as one had paper records having these under lock and key, literally, was sufficient security. However with the increasing use of the internet and cloud based systems, the ability to download large databases onto small devices has changed the way we should be thinking. The landscape has changed! There should be better supervision and accreditation of our PMS and audit of our EHR by our College through its Cornerstone Accreditation Programme. We expect that our Financial Institutions to implement the minimum Information Security Standards. We should expect no less form our health sector whether that be in public or private.

We should expect our General Practice College to insist on a minimum code of practice and work to up-skill our GP colleagues in achieving this standard over an acceptable negotiated timeframe. We should be insisting that PMS reach the ISO standard before they can implement further systems.

In particular we need to see mandated password security with a minimum character set and length. There should be forced password change after a defined period. There should be a timed lockout feature of any unattended portals. All system data needs internal mandatory backup and lastly validation of data inputs.

Despite all this we are required to be vigilant and constantly remind and audit our HCP from front desk staff or our General Practitioners about their critical role and obligation to maintain their patients' privacy and confidentiality by adhering to the recommendations of our IT security professionals.

If these HCP are less than diligent or choose to ignore these recommendations it could result in disclosure of information that not only harms the organisation's reputation but most importantly undermines the basis of the important doctor patient relationship-

Trust. We have ethical responsibilities to maintain our patients' secrets and confidences.

"The NZHIT Board wants GPs to lead the way in providing patients with secure online access to their health information." Having confidence in the security of information provided will be a key issue for organisations developing portals whereby the public can access their EHR (Robyn Nicholl, 2013).

In conclusion it is clear from this simple survey that many practices in New Zealand are operating PMS that do not comply with the minimum ISO standards which New Zealand has established for Information Security. We as a profession need to become more aware of our security responsibilities and put direct pressure on our PMS vendors to comply. We can do this at a Business level-i.e. from our General Practices, through our RNZCGPs and at a political level through such organisations as the NZHIT.

Bibliography

1993. Privacy Act. New Zealand.

CUSHMAN, R., FROOMKIN, A. M., CAVA, A., ABRIL, P. & GOODMAN, K. W. 2010. Ethical, legal and social issues for personal health records and applications. *Journal of Biomedical Informatics,* 43, S51-S55.

DR LAURENCE KNOTT. 2012. *Records, Computers and Electronic Health Record.* [Online]. Available: http://www.patient.co.uk/doctor/records-computers-and-electronic-health-record - ref-15 **[Accessed 11/06 2013].**

GIN GRAY. 13/06/2013 2013. *RE: RE: PMS software Security* Type to VERMUNT, S.

HEALTH AND DISABILITY COMMISIONER NEW ZEALAND 1996. The HDC Code of Health and Disability Services Consumers' Rights Regulation 1996.

IT HEALTHBOARD 2011. The Future of Health Enabled by Information.

JACOBS S, B. T. 2011. Placing the Next Pieces in New Zealand's EHR Jigsaw Puzzle. *HINZ.*

KLEIN C 2011. Cloudy Confidentiality: Clinical and Legal Implications of Cloud Computing in Health Care.

***J Am Acad Psychiatry Law,* 39, 571-578.**

MATASAR-PADILLA, M. 2012. *Lawyers and Cybersecurity: Preventing Breaches of Confidential Information* [Online]. Available: http://www.ethicalinvestigator.com/investigation/lawyers-and-cybersecurity-preventing-breaches-of-confidential-information/ **[Accessed 13/08/2012 2:55 PM.**

MEDICAL COUNCIL OF NEW ZEALAND 2001. The Maintanence and Retention of Patient Records. *In:* ZEALAND, M. C. O. N. (ed.) Amended October 2005 and August 2008 ed.

MOHAN P, K. S. 2011. Up in the Cloud: Ethical Issues that Arise in the Age of Cloud Computing. *Ethics & Professional Compensation Committee,* 8, 1.

NZMA 2011. Cole's Medical Practice in New Zealand 2011 *In:* GEORGE, I. S. (ed.) 10th ed.: Medical Council of New Zealand.

PRIVACY COMMISIONER 1994. Health Information Privacy Code1994. December 2008 ed.

RNZCGP 2011. The Practice Uses a Practice Management System. *In:* 2011, R. C. G. P. A. P. (ed.).

ROBYN NICHOLL 2013. National Health IT Board encourages GPs to take the lead. *Pulse*.

ROSS MONTGOMERY. 13/06/2013 2013. *RE: Incident #89132 - Survey questions.* Type to VERMUNT, S.

RYAN K M, B. A. J. 2004. Universal Electronic Health Records: A qualitative study of lay perspectives. *New Zealand Family Physician,* 31, 149-154.

ZETTER KIM. 2009. *Medical Records: Stored in the Cloud, Sold on the Open Market | Threat Level | Wired.com* [Online]. Available: http://www.wired.com/threatlevel/2009/10/medicalrecords/ [Accessed 13/08/2012 2:31 PM.

Appendix 1:

1. Access Control		Medtech	Houston	Profile
a. Do your PMS provide a means of authentication?				
i. What is your PMS mandated password length and minimum character set?				
ii. How often are the users forced to change their password?				
b. Do your PMS allow for specific area				

access rights?				
i. Do your PMS force password change on special function accounts that perform privileged functions? (E.g. Systems Administration, Security Administration etc.)				
c. Do your PMS have a timed lock-out/screen blanking function?				
d. Do your PMS have built in encryption protocols when information is copied or sent to disc or other medium?				
2. Orders and Recording				
a. Do your PMS use Ministry of Health HL7 protocols?				
b. Do your PMS support where applicable pre-coded data choice selections? (E.g. Radio buttons, check boxes, and/or drop boxes)				
c. Do your PMS support the recording and tracking of clinical orders and requests? (E.g. Laboratory orders, prescriptions, investigations.)				
3. Audit and Logging				
a. Do your PMS keep and audit of all transactions?				
b. Do your PMS date and stamp all entries?				
c. Do your PMS prevent the overriding of entries of a clinical nature?				
4. Backup				
a. Do your PMS have an automated backup procedure?				
b. Do your PMS have a built in data validation function?				
Other Comments:				
To whom are you accredited?				