Methods to Assess the Safety of Health Information Systems

Elizabeth Borycki and Elizabeth Keay

Abstract

Research has shown that the introduction of health information systems (HISs) can reduce the likelihood of medical errors. However, there is a growing body of evidence that suggests that if it is not designed or implemented properly, a HIS can actually cause or induce health professionals to make medical errors (i.e., technology-induced errors). In order to maximize the benefits of HISs while decreasing the likelihood of such inadvertent technology-induced error, it is important that we understand the range of methods that can be used to ensure the safety of our systems. In this article, we report the results of a review of the literature related to the methods used in predicting, preventing and evaluating the potential for a HIS to cause technology-induced error. These methods can be classified in terms of their application, including before a HIS is implemented, after a HIS has been implemented and after a technology-induced error has occurred.

In the early 1990s, the first studies were published that demonstrated that health information systems (HISs) could improve patient safety, leading the Institute of Medicine (1992) to conclude that some HISs, such as computerized physician order entry systems and decision support systems, can reduce medical errors. In the mid-2000s, there emerged research that documented the potential of some HIS features, functions and emergent workflows to introduce new types of medical errors into the clinical setting (Ash et al. 2007a; Ash et. al.2007b; Borycki and Kushniruk 2008; Horsky et al. 2005; Koppel et al. 2005; Kushniruk et al. 2005). Work by these researchers and others led some government agencies to ask healthcare organizations to proceed cautiously when implementing a HIS (e.g., Joint Commission 2008) and in other cases to implement new testing and certification procedures (e.g., Health Canada 2009). These publications signalled the need to develop new methods, approaches or techniques to: (1) detect technology-induced errors before a system is implemented and (2) identify the circumstances that contributed to a technology-induced error involving a HIS both during and after system implementation. Researchers developed these approaches in order to prevent any future technology-induced errors involving a HIS (Borycki et al. 2009). In this article, we review the current state of knowledge involving the key methods, approaches and techniques that can be used by healthcare administrators (e.g., chief information officers, chief executive officers, medical and nursing directors) to assess the safety of a HIS and its associated devices prior to their implementation in a healthcare organization.

Defining and Understanding Technology-Induced Errors

Technology-induced errors can be defined as those sources of error that may "arise from: (a) the design and development of a technology, (b) the implementation and customization of

a technology, and/or (c) the interactions between the operation of a new technology and the new work processes that arise from a technology's use" (Borycki and Kushniruk 2008: 154). Technology-induced errors have been referred to by some researchers as "e-iatrogenesis" (Sittig 2008) and by others as one type of "unintended consequence" (Ash et al., 2007a; Ash et al., 2007b; Borycki et al. 2010, September). They differ from medical errors and adverse events as described by Classen and others (e.g., Classen and Metzger 2003; Kilbridge and Classen 2001). *Medical errors* can be defined as "failures in the process of medical management … that have potential to harm the patient," and *adverse events* can be defined as those events arising from medical management that lead to patient harm or injury (Classen and Metzger, 2003: 42).Technology-induced errors have their origins in the technology itself and technology-human interactions, rather than the entire medical management process. Therefore, technology-induced errors may be considered one type of unintended consequence or error arising from the design, development, implementation and customization of technology and from the new workflows and interactions between technology and health professionals that emerge from a technology's use during the process of providing healthcare (Borycki et al. 2010, September).

Figure 1. Continuum of methods for diagnosing technology-induced error

HIS = health information system.

To develop a comprehensive review of the current methods, approaches and techniques used to diagnose technology-induced error, we conducted a search of Medline using the following key search terms: *technology induced error* and *method*, *technology induced error* and *technique*, *technology induced error* and *approach*, *unintended consequences* and *method*, *unintended consequences* and *technique*, *unintended consequences* and *approach*, *e-iatrogenesis* and *method*, *e-iatrogenesis* and *technique*, and *e-iatrogenesis* and *approach*. In our search of Medline, we identified 174 publications of which 13 abstracts described methods, techniques and approaches that could be used to identify potential and actual sources of technology-induced error in healthcare. There exist a number of methods published in the health informatics literature that can be used to determine the safety of a HIS during its design, development and procurement, prior to its implementation.

Here we describe and discuss these methods, approaches and techniques in terms of their relevance to healthcare administrators as part of an organization's risk management strategy. The methods are discussed in terms of a continuum that can be used by healthcare administrators from HIS software development (testing software and devices during the software design, development, procurement and pre-implementation processes) through to implementation and maintenance in clinical settings (Figure 1). In addition, each of these methods is described and reviewed in terms of its potential use in healthcare organizations (e.g., software vendors, hospitals and regional health authorities) as part of an organizational risk management strategy.

Before HIS Implementation: Design, Development, Procurement and Pre-implementation Processes

Safety Heuristics

The use of evidence-based heuristics to evaluate the safety of software is a relatively new phenomenon. Historically, heuristics were developed and used to evaluate the usability of a HIS interface design (Kushniruk and Patel 2004). More recently, Carvalho and colleagues (2009) developed a list of evidence-based heuristics (i.e., guidelines regarding safe design) that could be used to evaluate the safety of HIS interface features, functions and emergent workflows during the software procurement process. These safety heuristics were developed and tested in three phases. In phase one, the researchers conducted a systematic review of the published literature on technology-induced error. In phase two, three health informatics experts generated a set of heuristics during a round-table discussion after reviewing the evidence-based literature. The round-table discussion identified heuristics, which were classified into four safety domains: content, functions, workflows and safeguards. In phase three, the safety heuristics were applied to a demonstration version of the Veterans Affairs Computerized Patient Record System. This involved an analyst comparing features of the system and user interface against the set of heuristics and noting conformance or violation of the heuristics, as could be done by an analyst evaluating a system being considered for purchase by a regional health authority. The researchers found that 12 of the developed heuristics could be readily applied by an analyst conducting

this type of evaluation. However, the researchers suggested that the remaining heuristics could be applied in conjunction with clinical simulation testing (Carvalho et al. 2009).

Use of Clinical Simulations

Several researchers have explored the use of clinical simulations as a methodology for identifying potential sources of technology-induced error arising from human-computer interaction. Clinical simulations typically involve observing health professionals interacting with the system (e.g., an electronic health record system or medication administration systems) using representative devices (e.g., a workstation or wireless cart) in a typical workplace (e.g., a hospital room) while they carry out representative real-world tasks (e.g., entering medication orders or performing medication administration) (Kushniruk et al. 2005, 2006).

Clinical simulations involve analysts video recording health professionals' interactions with a HIS and its associated devices. Computer screen recordings are also made to observe how the health professionals perform work-related tasks using the HIS. Subsequently, the analyst interviews the health professionals about the difficulties they may have experienced in using the software and hardware. The analyst then reviews the interview, video and audio data to identify instances of technology-induced errors (i.e., mistakes) and near misses (i.e., slips) (Kushniruk et al. 2005). This information is used to make modifications to the HIS, the types of devices that are used and the organization's policies, procedures and training to prevent any future occurrence of technology-induced errors or near misses (Kushniruk et al. 2006; Kuwata et al. 2006). It is worthwhile to note that these types of simulations, that is, those focused on technology-induced errors, differ from those simulations conducted to determine the ability of a HIS to detect human data-entry errors, such as the simulations used to certify computerized physician order entry (CPOE) systems. Simulations that are used to certify CPOE systems involve simulated patients and orders to assess the ability of a CPOE system to detect adverse events and errors made by the health professionals entering the orders (e.g., physicians, nurse practitioners) (Classen et al. 2007). The focus of this latter type of simulation is on human error detection, such as assessing the ability of a system to notice human errors in prescribing (Classen et al. 2007), rather than on the error-inducing qualities of the HIS (Borycki et al. 2010, September; Kushniruk et al. 2005).

A Japanese and a US healthcare organization used clinical simulations to identify potential sources of technology-induced error before implementing a medication administration system and physician order entry system on a large scale (see Kushniruk et al. 2005; Kuwata et al. 2006). These clinical simulations provided HIS and device implementers in these hospital settings with system-specific feedback to prevent the occurrence of errors.

Clinical plus Computer-Based Simulations

More recently, clinical simulation work has been extended to include the use of computer-based simulations involving computer modelling to provide healthcare decision-makers with information about the potential impact of a HIS and its associated devices where technology-induced errors are concerned at a regional health authority level (Borycki et al. 2009). Data from clinical simulations were used as input parameters to a computer-based simulation model and extended to provide decision-makers with information about the impact of these technology-induced errors upon organizational medication error rates (i.e., physicians making prescribing errors as a result of interface design features) over time, such as over a year. In this work, the researchers have shown that if left unaddressed, technology-induced errors may have a significant impact upon organizational error rates. Such information may help decision-makers to identify those technology-induced errors that might have the greatest impact upon the organization and enable them to develop a risk management strategy that includes interventions aimed at preventing the likelihood of an error occurring, such as redesigning some aspects of the HIS interface features and functions, selecting another device that better supports health professional work or altering the content of health professional training to ensure that health professionals are aware of how the system works (Borycki et al. 2009).

After HIS Software Implementation: Ethnography

A number of studies (e.g., Koppel et al. 2005) have documented the utility of ethnographic approaches such as interviews, focus groups, surveys and observations of health professionals using HIS in the study of technology-induced error after HIS implementation. Ethnographers have used varying combinations of these data-collection methods to document potential sources of technology-induced error (e.g., Ash et al., 2007a; Ash et al., 2007b; Koppel et al. 2005). Interview and focus group data gathered from physicians and nurses have been used to identify many instances where a HIS could lead to an error. The findings from these studies were significant; they suggest that health professionals could identify potential error-facilitating properties of a HIS or device while working in a clinical setting. These studies also signalled a need for governments and regional health authorities to develop error-reporting systems that allow health professionals to provide details about their real-world near-miss and error experiences involving HISs and devices.

Although ethnographic approaches can help to identify technology-induced errors, other research has found that health professionals may not be aware of the error-inducing aspects of a HIS and are therefore unable to report their occurrence (see Kushniruk et al. 2005). This research suggests that ethnographic approaches may have value in detecting some types of

errors but that a group of technology-induced errors may go undetected by both the health professionals who are involved in near misses and errors and the ethnographers who are gathering data from health professionals using these systems (Borycki and Kushniruk 2008; Kushniruk et al. 2005). Health professionals may not be able to recall the instances where a potential or actual error may have occurred or the events that led to that error (i.e., recall bias) (Jackson and Verberg 2007). Furthermore, in cases where there is an external observer (such as an ethnographer), sometimes not all the technology-induced errors are recorded (i.e., ethnographers are sometimes physically unable to record all of the relevant data from health professional interactions with HISs) or the observers focus on only the activities they identified as relevant at the outset of their work (i.e., recording bias) (Jackson and Verberg 2007).

Costs associated with making modifications to the system, re-implementation and re-training health professionals would be significantly reduced if changes were made to the system prior to implementation.

Another weakness of using ethnography after a system is in use in a clinical setting is the amount of time required to collect the data (e.g., several months of intensive work; Ash et al. 2007a; Ash et al., 2007b). Some researchers have attempted to reduce the amount of time needed to collect data about a HIS – as a result, a modified version of ethnography known as Rapid Assessment of Clinical System Interventions (RACSI) has been developed (Ash et al. 2008, November 6). Like ethnography, RACSI utilizes interviews, surveys and observations of health professionals using a HIS. Data collection and analysis take up to one month to complete (Ash et al. 2008, November 6). Although this is an improvement over traditional ethnographic approaches, errors may occur during the one-month period of data collection and analysis. Lastly, ethnographic and RACSI approaches to identifying technology-induced errors may lead to increased costs for regional health authorities, such as those associated with making modifications to the system, re-implementation and re-training health professionals. These costs would be significantly reduced if changes were made to the system prior to implementation (Kaner et al. 1999; Patton 2001).

After an Error Has Occurred

A case study approach has been used by a group of cognitive experts at a large teaching hospital in the United States to determine the root causes of errors and to identify any potential causes of errors involving "failures in the interaction between humans and information systems" (Horsky et al. 2005: 377). Cognitive experts investigated an error that resulted in a patient being found severely hyperkalemic; they first developed a timeline for events that led to the error using computer log data, performed an expert review of computer order entry, transfer and sign-out notes screens and then interviewed the two physicians involved in the error. The outcomes of the review were significant. The experts were able to identify the factors that contributed to the errors such as "errors by physicians in the use of the clinical information system, the absence of automated safeguards that help prevent errors, and uncertainty on the part of physicians about how to manage unusual ordering scenarios" (Horsky et al. 2005:308). The experts made several recommendations that could be implemented at vendor and organizational levels for error prevention, including (1) some modifications to the computer screen designs, (2) the introduction of alerts to inform users if the patient is already receiving the medication and if an order for a medication requires a review of more recent laboratory tests results and (3) further training for clinicians (Horsky et al. 2005).

Lessons Learned

In our work, we have identified several approaches to identifying technology-induced error from HIS development though to implementation. In our search of Medline, there emerged a number of methods that may be used to test for or diagnose potential causes of technology-induced error. These include (1) the use of evidence-based heuristics to evaluate the safety of a HIS, (2) the use of clinical simulations to identify technology-induced error interactions between a HIS/devices, health professionals and patients, (3) an extension of clinical simulations to include computer-based simulations to observe long-term organizational implications of errors if uncorrected, (4) the use of ethnography after a HIS has been implemented, (5) an extension of ethnography referred to as rapid assessment and (6) the use of case studies after a technology-induced error has occurred. It is worthy to note that a failure modes and effects analysis (FMEA) was not reported from the literature search as being employed by health informatics researchers to identify potential technology-induced errors, nor was the method reported in the literature as being used to determine the factors that contributed to a technology-induced error that has occurred. To better understand the possible underlying reasons for this, one must consult the FMEA and healthcare FMEA literature.

FMEA was developed by reliability engineers to predict system reliability to establish the overall probability that a system will operate for a specific length of time without a component failure (Leveson 1995). In engineering, FMEA does not consider the effects of multiple failures and human error in operating procedures – that is, each failure is reviewed as an independent event, so this technique does not capture the interrelationships among system elements (Leveson 1995). FMEA

is used in safety analysis because it looks at the end effects of failure; but not all failures result in accidents, so FMEA can be inefficient (Leveson 1995). In healthcare, FMEA is used as a risk management tool to identify and control risks beyond the HIS. Healthcare FMEA is considered to be a proactive and thorough risk-control tool that allows for the examination of a process to determine what could go wrong. Healthcare FMEA uses the following steps (Leigh and Lagorio 2006):

1. Select a high-risk process to study.
2. Assemble an interdisciplinary team.
3. Diagram and describe the processes and sub-processes.
4. Brainstorm to identify all the failure points.
5. Identify the causes of failure using brainstorming and incident reports, their probability and severity to create a risk matrix.
6. Develop and implement actions with a responsible person.
7. Assess to ensure no new failure modes have been created.

These risk reduction actions must accomplish at least one of the following three objectives in order to be considered effective and to avoid future iterations of the FMEA process: (1) remove a single-point weakness, (2) create one or more effective control measures or (3) make the hazard so obvious that control measures are not needed (Grout 2007). FMEA can also be used to assess new programs, services or departments (Cohen and Tuohy 2006).

This review of the literature revealed that FMEA and healthcare FMEA were not specifically used by health informatics researchers to predict or prevent technology-induced errors, despite the fact that FMEA is used in safety analysis in healthcare (Leveson 1995). There may be a number of reasons for this. According to Classen and Metzger (2003), in healthcare, FMEA is primarily used to study sentinel adverse events, which differ from technology-induced errors (i.e., learning about the factors or flaws in a healthcare system that lead to an adverse event during medical management versus learning about how technology induces an error). The advantages of FMEA are its systematic approach, ability to build teams and promote teamwork, act as a visibility tool for managers, identify potential concerns and improve user satisfaction (Dhillon 2008; Leveson 1995). Its disadvantages include the time and costs involved in its use (Grout 2007; Levenson 1995). As well, FMEA, when applied to understanding adverse events in healthcare, does not provide sufficient information about the frequency of an adverse event, describe the relative contribution of differing factors or flaws in the HIS that lead to an adverse event or provide explicit prescriptive information about what action to take (Grout 2007; Leveson 1995). Instead, FMEA focuses on rare events and identifies a list of flaws with the current healthcare system (Classen and Metzger 2003).

Modifications to a HIS can be costly (especially after it has been fully developed or implemented) (Kaner et al. 1999; Patton 2001). Identifying technology-induced errors, understanding the frequency of their occurrence and the relative contributions of specific aspects of the design, development and implementation of a HIS that contribute to technology-induced errors will allow decision-makers to determine the system's impacts on healthcare (Borycki and Kushniruk 2008; Borycki et al. 2009). Such information, made available prior to full-scale system deployment, is necessary for decision-makers to assess risks and determine if fundamental changes to the software are necessary. FMEA (as has been applied in this area of healthcare) does not provide this information, whereas approaches in the literature regarding technology-induced errors do provide such information. For example, clinical simulations can be used to identify the types of technology-induced errors that are present and their relative frequency. Computer-based simulations can be used to determine the relative costs of addressing a technology-induced error versus the costs of patient injury and death over time at a healthcare system level (Borycki et al. 2009). Future research will need to investigate the utility of using FMEA in healthcare to manage risks associated with technology-induced error.

Summary

Regional health authorities are increasing their investment in HISs as a way of improving the effectiveness and efficiency of the healthcare system while at the same time reducing medical error rates. With the implementation of a HIS, new types of errors have been introduced into the healthcare system (i.e., technology-induced errors). These errors need to be addressed. In this article, we have presented a range of literature-documented methods, techniques and approaches to address technology-induced errors as part of a healthcare organizational risk management strategy. Healthcare administrators can use these methods in differing ways. Safety heuristics and clinical simulations can be used during the procurement process to identify systems for purchase according to their safety attributes. Clinical simulations can be used by healthcare organizations to identify potential technology-induced errors (near misses and mistakes) within the context of a safe simulated environment before implementation in the real world. Clinical simulations plus computer-based simulations can help healthcare administrators to identify those risk management activities involving a HIS (e.g., screen re-design, extra training for health professionals) they would like to undertake based on the HIS features and functions that may lead to error. Ethnography and RACSI allow health administrators to identify potential technology-induced errors after a system has been implemented. Lastly, case studies can be effectively used to identify the factors that have led to an error, and provide healthcare administrators with recommendations that would prevent errors from occurring. In

summary, there are a number of methods that can be used by healthcare organizations to address technology-induced error as part of an organization's risk management strategy. HQ

References

Ash, J.S., D.F. Sittig, C.K. McMullen, K. Guappone, R. Dystra and J. Carpenter. 2008, November 6. "A Rapid Assessment Process for Clinical Informatics Interventions." *AMIA Annual Symposium Proceedings* 26–30.

Ash, J.S., D.F. Sittig, E.G. Poon, K. Guappone, E. Campbell and R.H. Dykstra. 2007a. "The Extent and Importance of Unintended Consequences Related to Computerized Provider Order Entry." *Journal of the American Medical Informatics Association* 14(4): 415–23.

Ash, J.S., D.F. Sittig, R.H. Dykstra, K. Guappone, J.D. Carpenter and V. Seshadri. 2007b. "Categorizing the Unintended Sociotechnical Consequences of Computerized Provider Order Entry." *International Journal of Medical Informatics* 76S: S21–27.

Borycki, E.M., A. Kushniruk, E. Keay, J. Nicoll, J. Anderson and M. Anderson. 2009. "Toward an Integrated Simulation Approach for Predicting and Preventing Technology-Induced Errors in Healthcare: Implications for Healthcare Decision-Makers." *Healthcare Quarterly* 12: 90–96.

Borycki, E.M. and A.W. Kushniruk. 2008. "Where Do Technology-Induced Errors Come From? Towards a Model for Conceptualizing and Diagnosing Errors Caused by Technology." In A.W. Kushniruk and E.M. Borycki, eds., *Human, Social and Organizational Aspects of Health Information Systems.* Hershey, PA: IGI Global.

Borycki, E.M., A.W. Kushniruk, C.J. Carvalho and M.-H. Kuo. 2009, November. *A Systematic Review of Qualitative and Quantitative Methods Using to Identify and Study Technology-Induced Errors in Computerized Physician Order Entry (CPOE).* Presented at the Asia Pacific Association of Medical Informatics Conference, Hiroshima, Japan.

Borycki, E.M., A.W. Kushniruk and J. Brender. 2010. September. *Theories, Models and Frameworks for Diagnosing Technology-Induced Errors.* Presented at the MedInfo Conference, Capetown, South Africa.

Carvalho, C.J., E.M. Borycki and A.W. Kushniruk. 2009. "Ensuring the Safety of Health Information Systems: Using Heuristics for Patient Safety." *Healthcare Quarterly* 12: 48–51.

Classen, D.C., A.J. Avery and D.M. Bates. 2007. "Evaluation and Certification of Computerized Provider Order Entry Systems." *Journal of the American Medical Informatics Association* 14(1): 48–55.

Classen, D.C. and J. Metzger. 2003. "Improving Medication Safety: The Measurement Conundrum and Where to Start." *International Journal of Quality in Health Care* 15(1): 41–47.

Cohen, H. and N. Tuohy. 2006. "The Risk Management Professional and Medication Safety." In R. Carroll and S.M. Brown, eds., *Risk Management Handbook, Volume II: Clinical Risk.* San Francisco: Jossey Bass.

Dhillon, B.S. 2008. *Reliability Technology, Human Error and Quality in Health Care.* Boca Raton, FL: CRC Press.

Grout, J. 2007. *Mistake-Proofing the Design of Health Care Processes* (Publication No. 07-0020). Rockville, MD: Agency for Healthcare Research and Quality.

Health Canada. 2009. *Classification of Medical Devices Class I or Class II Patient Management Software.* Ottawa, ON: Author. Retrieved January 25, 2010. <http://www.hc-sc.gc.ca/dhp-mps/md-im/activit/announce/md_notice_software_im>.

Horsky, J., G.J. Kuperman and V.L. Patel. 2005. "Comprehensive Analysis of a Medication Dosing Error Related to CPOE." *Journal of the American Medical Informatics Association* 12(4): 377–82.

Institute of Medicine. 1992. *To Err Is Human: Building a Safer Health System.* Washington, DC: National Academy Press.

Jackson, W. and N. Verberg. 2007. *Methods: Doing Social Research.* Toronto, ON: Pearson.

Joint Commission. 2008. *Sentinel Event Alert: Safely Implementing Health Information and Converging Technologies.* Oakbrook Terrace, IL: Author. Retrieved January 25, 2010. <http://www.jointcommission.org/SentinelEvents/SentinelEventAlert/sea_42.htm>.

Kaner, C., J. Falk and H.Q. Nguyen. 1999. *Testing Computer Software* (2nd ed.). Toronto, ON: Wiley.

Kilbridge, P. and D.C. Classen. 2001. "Surveillance for Adverse Drug Events: History, Methods and Current Issue." *Research Series* 3: 1–35.

Koppel, R., P. Metlay, A. Cohen, B. Abaluck, A.R. Localio, S.E. Kimmel et al. 2005. "Role of Computerized Physician Order Entry Systems in Facilitating Medication Errors." *Journal of the American Medical Association* 293(10): 1197–203.

Kushniruk, A., E. Borycki, S. Kuwata and J. Kannry. 2006. "Predicting Changes in Workflow Resulting from Healthcare Information Systems: Ensuring the Safety of Healthcare." *Healthcare Quarterly* 9(Special Issue): 114–18.

Kushniruk, A.W., M.M. Triola, B. Stein, E.M. Borycki and J.L. Kannry. 2005. "Technology Induced Error and Usability: The Relationship between Usability Problems and Prescription Errors When Using a Handheld Application." *International Journal of Medical Informatics* 74(7–8): 519–26.

Kushniruk, A.W. and V.L. Patel. 2004. "Cognitive and Usability Engineering Methods for the Evaluation of Clinical Information Systems." *Journal of Biomedical Informatics* 37(1): 56–76.

Kuwata, S., A. Kushniruk, E. Borycki and H. Watanabe. 2006. "Using Simulation Methods to Analyze and Predict Changes in Workflow and Potential Problems in the Use of a Bar-Coding Medication Order Entry Systems." *AMIA Annual Symposium Proceedings* 994.

Leigh, J. and N. Lagorio. 2006. "Clinical Crisis Management." In R. Carroll and SM. Brown, eds., *Risk Management Handbook, Volume II: Clinical Risk.* San Francisco: Jossey Bass.

Leveson, N. 1995. *Saferware. System Safety and Computers.* Boston: Addison Wesley.

Patton, R. 2001. *Software Testing.* Indianapolis, IN: SAMS.

Sittig, D.F. 2008. "A Socio-Technical Model of Health Information Technology-Related E-iatrogenesis." *AMIA Annual Symposium Proceedings* 1209–10.

About the Authors

Elizabeth Borycki, RN, PhD, is an assistant professor in the School of Health Information Science at the University of Victoria, Victoria, British Columbia, Canada. Her email address is emb@uvic.ca.

Elizabeth Keay, MD, FRCPC, CRM, is a PhD student, School of Health Information Science, University of Victoria.