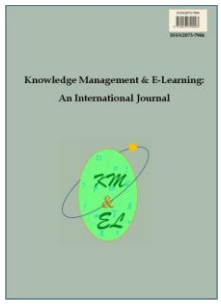
**Knowledge Management & E-Learning**




ISSN 2073-7904

# Towards a framework for teaching about information technology risk in health care: Simulating threats to health data and patient safety

**Elizabeth M. Borycki**
University of Victoria, Victoria, Canada

**Recommended citation:**
Borycki, E. M. (2015). Towards a framework for teaching about information technology risk in health care: Simulating threats to health data and patient safety. *Knowledge Management & E-Learning*, *7*(3), 480–488.

*Knowledge Management & E-Learning, 7(3), 480–488*

# Towards a framework for teaching about information technology risk in health care: Simulating threats to health data and patient safety

Elizabeth M. Borycki*

School of Health Information Science
University of Victoria, Victoria, Canada
E-mail: emb@uvic.ca

*Corresponding author

**Abstract:** In this paper the author describes work towards developing an integrative framework for educating health information technology professionals about technology risk. The framework considers multiple sources of risk to health data quality and integrity that can result from the use of health information technology (HIT) and can be used to teach health professional students about these risks when using health technologies. This framework encompasses issues and problems that may arise from varied sources, including intentional alterations (e.g. resulting from hacking and security breaches) as well as unintentional breaches and corruption of data (e.g. resulting from technical problems, or from technology-induced errors). The framework that is described has several levels: the level of human factors and usability of HIT, the level of monitoring of security and accuracy, the HIT architectural level, the level of operational and physical checks, the level of healthcare quality assurance policies and the data risk management strategies level. Approaches to monitoring and simulation of risk are also discussed, including a discussion of an innovative approach to monitoring potential quality issues. This is followed by a discussion of the application (using computer simulations) to educate both students and health information technology professionals about the impact and spread of technology-induced and related types of data errors involving HIT.

**Keywords:** Health information technology; Health information systems; Information technology risk; Health informatics; Data integrity; Data quality; Data safety; Risk management; Data security; Technology induced errors; Simulation

**Biographical notes**: Dr. Elizabeth Borycki, RN, PhD is an Associate Professor with the School of Health Information Science at the University of Victoria in Victoria, British Columbia, Canada. Dr. Borycki's research interests include health information systems safety, human factors, clinical informatics, organizational behavior and change management involving health information systems. Elizabeth has authored and co-authored numerous articles and book chapters as well as edited several books examining the effects of health information systems upon health professional work processes and patient outcomes. Dr. Borycki is also the Vice Chair of the Health Informatics for Patient Safety Working Group for the International Medical Informatics Association.

## 1. Introduction

The worldwide proliferation of electronic health data and its interchange has led to concerns about data quality, security, safety and accuracy as ever greater amounts of such data are rapidly being stored, transmitted and exchanged (Perakslis, 2014). In this paper the author first: (a) describes an information technology risk framework, and (b) outlines how the framework can be used to educate health professionals to proactively ensure that electronic data is accurate, useful and free from corruption from any number of sources. The approach described in this paper is a layered framework that considers data risk management broadly in such a way as to mitigate risk of incorrect or inaccurate health data being used in healthcare decision making. The sources of such incorrect data may be many and varied, including inadvertently introducing error due to human factors issues (Borycki & Kushniruk, 2005), technological problems due to interoperability and exchange issues (Kushniruk, Surich, & Borycki, 2012), or the presence of technology-induced error (Kushniruk, Triola, Borycki, Stein, & Kannry, 2005).

In addition, error may result from other sources and incorrect data that may affect patient safety. These types of errors may arise from intentional or nefarious causes (e.g. as the result of intrusions, hacking or malware) (Sametinger, Rozenblit, Lysecky, & Ott, 2015). In this paper the author argues that an integrated framework towards information technology risk management will ensure health data quality and integrity (regardless of the source) and will be an important direction to follow in educating health professionals into the future. Along these lines, prior work in the area of detecting and preventing unintentional sources of error (what has been termed as "technology-induced error") has highlighted the need to develop frameworks for dealing with such errors to reduce risk and to educate health professionals about these potential risks. However, to date, frameworks for educating health professionals about mitigating these types of risks due to this type of error have been limited. Instead, some research has led to the development of frameworks that can be used by technology developers to identify these types of risks (Borycki, Kushniruk, Bellwood, & Brender, 2012). Other research has focused on developing frameworks for mitigating risk caused from intentional sources such as security breaches and malware in health care (Coronado & Wong, 2014). Much can be learned and shared in considering the research on broader frameworks for risk of missing or inaccurate health data in general, be the sources of that risk be technology or people (human factors issues), or alternatively, from intentional nefarious sources.

In this paper the author proposes an information technology risk framework and outlines how the framework can help health professionals learn about the importance of data quality, safety and integrity. Such knowledge is important from a health professional perspective and an ultimate concern for patient safety as these data are used in health professional decision making regarding diagnosis, treatment and management of disease and needs to be reflective of the patient's health condition. Health professionals need to be aware of these sources of information technology risk. They need to identify possible data quality, safety and integrity issues so that health information technology professionals can model, find solutions to and mitigate these types of issues.

## 2. Towards an information technology risk framework

Technologies should both protect the privacy of information and ensure the integrity, quality and safety of the data they store, accumulate and generate. Ultimately, if health data is corrupted either intentionally or unintentionally, when such errors occur, it is a serious patient safety issue that must be detected, mitigated, properly sourced and

addressed (Borycki & Kushniruk, 2005; Institute of Medicine, 2011). Recurring patterns of threats to data integrity need to be identified, modeled and mitigated using long term solutions. In health care the accuracy of patient data is critical. Such data can be considered in the context of a number of different levels in order to ensure that the data is secure and free from unintended alteration. As will be discussed in subsequent sections of this paper, many of the safeguards that can be considered in ensuring that data is secure can also be extended to help ensure that data is correct, unaltered, accurate and safe to use (as these are parallel goals). Fig. 1 shows the 6 levels of the framework that will be discussed in this paper with data integrity, including both risks from intentional and unintentional alterations of health data and error. These levels are described below.

**Level 1 – Human factors and usability**

To ensure both the quality of health data and the usability of health information technologies one must consider technology within the context of a number of perspectives (see Fig. 1, Level 1). These include human factors and usability perspectives. Human factors refers to the study of the "understanding of interactions among humans and other elements of a system, and the profession that applies theory, principles, data and methods to design in order to optimize human well-being and overall system performance" (International Ergonomics Association, 2015) (http://www.iea.cc/whats/) while usability refers to measures of ease of use and usage of health information technology. Usability also includes concepts such as the learnability of the technology, its effectiveness and efficiency in supporting health professional work, aspects such as user enjoyment while using the technology and safe use of a health information systems (Preece et al., 1994). In previous work Kushniruk and colleagues (2005) found that unusable systems may be a source of high risk in leading to technology-induced errors, resulting in the storage and/or access of incorrect patient data that might be used by health professionals in patient related decision-making. For example, if a drop down menu in an e-prescribing system automatically populates a field with a default value rather than the value that was entered by a clinician then the wrong dosage of a medication may be given to a patient (Borycki & Kushniruk, 2005; Kushniruk et al., 2005). Another example of a technology-induced error that has been noted in the research literature involves the use of electronic health records in hospitals. Electronic health records are used to document patient information and allow for communication between health professionals caring for a patient. Electronic health record systems that allow multiple patient records to be open on one computer screen at the same time may lead to error if a busy clinician is called away for an emergency, and then later returns to the computer and then inadvertently enters data into the wrong open patient record (Bowman, 2013). This technology-induced error can then be easily propagated throughout an entire networked healthcare system and then across interoperable systems (Bowman, 2013; Kushniruk, Surich, & Borycki, 2012).

From the security and privacy side, systems should be usable in that they should not require memorization of an excessive number of passwords, security measures and checks. The design of security and privacy systems for health information technologies used in the process of providing health care to patients should not make it difficult for health professionals to easily access and use these technologies when caring for patients (especially patients that are experiencing a health crisis). To mitigate against such risk, a layered approach to usability testing has been recommended, which includes testing systems prior to widespread implementation by applying standard usability tests, followed by clinical simulations to ensure accuracy and integrity of data entered into the systems (Kushniruk, Nohr, Jensen, & Borycki, 2013).

**Level 2 – Monitoring security and accuracy of data**

Whether health data has been corrupted or made inaccurate by intentional or unintentional means, the automated and accurate monitoring of health data will become a critical issue as the amount of health data transmitted and stored electronically increases exponentially. Studies have shown that an increase in transmission of medication data across many systems also greatly increases the chance for error (e.g. through scrambled networked messages, transmission and other errors) (Ö hlund, Å strand, & Petersson, 2011). In addition to this, data may be corrupted or redirected through nefarious causes such as malware and worms. To deal with this, healthcare network monitoring software will need to be extended to include triggers and rules for detecting such problems (Kushniruk, Surich, & Borycki, 2012). Malicious software protection mechanisms need to be deployed and integrated with network monitoring in identifying weaknesses in an organization's health network that may lead to storage, transmission and propagation of erroneous patient data. Such work represents a second layer of information technology risk that needs to be understood and considered (see Fig. 1, Level 2).

**Level 3 – HIT architectural controls**

At the architectural level, the building in of capabilities for redundancy, regular back-up, effective and rapid recovery from attack and the ability to isolate and cut off unreliable or negatively affected subsystems are all critical to ensure the integrity of the data contained within a healthcare system. The considerations regarding architecture apply when one is considering potential errors from any number of sources, including both intentional and unintentional sources. Once error has been detected then safeguards must be put in place to prevent further error propagation within networked healthcare systems (see Fig. 1, Level 3).

**Level 4 – Operational and physical checks**

At the operational level (see Fig. 1, Level 4), there are a number of considerations and issues that need to be considered to ensure the safety, quality and integrity of health data, particularly as such data becomes more integrated and interchanged across systems. Considerations here include security operations management, the comprehensiveness of business agreements among organizations sharing health data, education and training to support proper use of systems and identification of problems with data transmission, integrity and quality.

**Level 5 – Healthcare data quality assurance policies**

At the healthcare quality assurance level (See Fig. 1, Level 5), policies must be constructed that govern operation of technology, information exchange and continuous evaluation of data quality. For example, in the United States the Health Insurance Portability and Accountability Act (HIPAA) protects the confidentiality and security of health information (HIPPA, 1996). HIPPA provides standards for physically safeguarding health data (HIPPA, 1996) while in Canada acts such as the Freedom of Information and Protection of Privacy Act (FIPPA) in the province of British Columbia deals with similar regulation (Office of the Information and Privacy Commissioner for British Columbia, 2015). The area of policy for ensuring health data quality in terms of specifying how data can be ensured to be free from sources of error such as technology-induced error is currently a new area with the promise of regulatory control which is still lacking in Canada and the United States (Institute of Medicine, 2011; Kushniruk, Bates, Bainbridge, Househ, & Borycki, 2013).

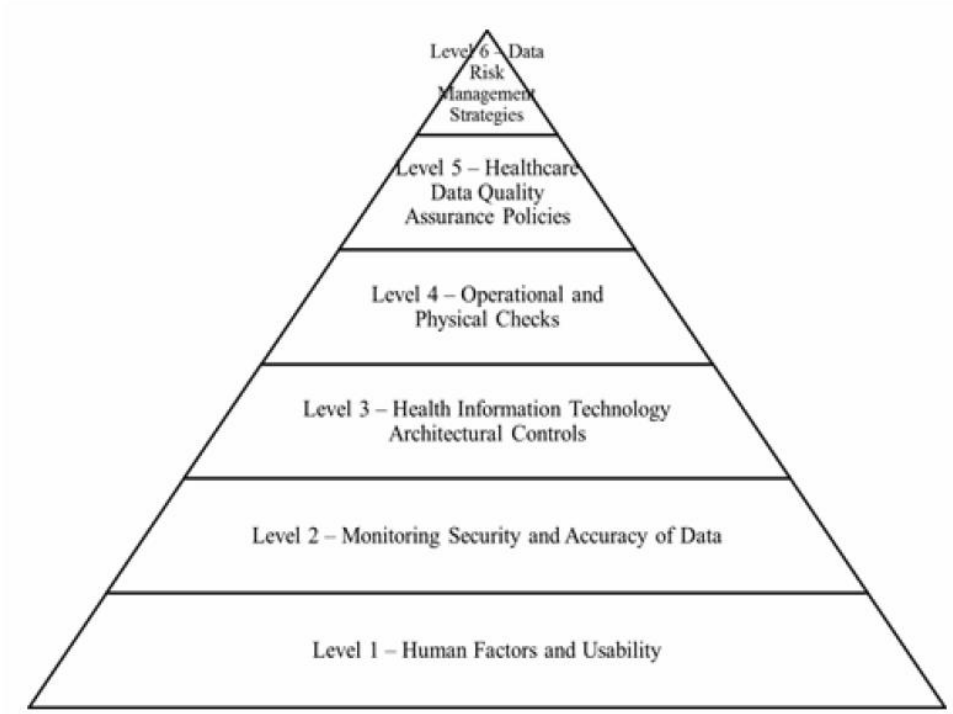



**Fig. 1.** Information technology risk in healthcare framework

**Level 6 – Data risk management strategies**

Lastly, an overall risk management strategy needs to be put into place in organizations to allow for a top level of integration and mitigation of risk associated with the creation and propagation of incorrect or inaccurate health data throughout an organizations' network and through interoperability protocols to other organizations (see Fig. 1, Level 6). This strategy should build on the previous layers described above and should drive the continual evaluation of the safety and quality of health data in an organization. Along these lines, a number of standards for risk management have appeared, such as International Standards Organization (ISO) standards for risk management, and the principles of the risk management cycle are being applied more widely, including application of risk identification, assessment, prioritization, mitigation and monitoring (ISO, n.d.).

## 3. Monitoring and simulation of health information technology risks in health care

Previous research in modeling technology-induced errors in health care has focused on modeling the spread and propagation of error (e.g. medication error) arising as the result of technology-induced error. This work involved collecting base rates on the occurrence of a range of types of data errors that were obtained from conducting usability and simulation studies. The data came from video based observational studies of physicians entering data into a handheld mobile application (Borycki, Kushniruk, Anderson, &

Anderson, 2010; Borycki et al., 2009). The video recordings of the user interactions over time were analyzed to detect the presence of technology-induced error and determine base rates for such error. These base rate data were then fed into a dynamic simulation model developed using the Stella dynamic simulation and modeling tool (Kushniruk et al., 2005). The study showed how varying parameters of the underlying simulation model (corresponding to parameters from each of the 6 levels of the framework in Fig. 1) affected propagation of error, if errors were allowed to spread across hospital systems. For example, at Level 1, particular features of the applications user interface (i.e. problematic user interface features) were modified, leading to a reduction in different types of usability and human factors problems and ultimately a reduction in technology-induced errors over time (Borycki et al., 2009). At Level 4, in the simulation model different features of operational safeguards were modified to explore the impact of different levels of error detection when sharing information across organizations. The other levels of the framework described above were used to explore different aspects of error detection using different mitigation strategies (Kushniruk, Borycki, Anderson, & Anderson, 2009). We are currently modifying the underlying simulation models to explore the impact of errors generated from intentional sources (e.g. from hacking and malware) in the same manner. To date, the framework described above has proved useful to the analysis of a range of health data error types and we are currently working on developing an ontology of errors and error patterns that includes consideration of both unintentional and intentional errors, with each of these classes of errors being decomposed into subclasses of error (Kushniruk et al., 2005; Kushniruk & Borycki, 2015).

## 4. Threat modeling and simulations for training health professionals

In the computer industry threat modeling is rapidily becoming a critical emerging area as risk of both unintended and intentional threats to data security and accuracy increase with the exponential rise in interoperable and connected systems (Kushniruk, Surich, & Borycki, 2012). Nowhere is this more of a concern than in the health information technology era, with the increased digitization of health data and increasing interconnectivity across healthcare settings (Borycki, Lemieux-Charles, Nagle, & Eysenbach, 2009) . The simulations and information technology risk in the healthcare model described in previous sections of this paper can be used to provide both a way of training health profesionals as well as a mechanism for decision support for management to identify and respond to data integrity breeches. Such an approach to providing training in threat modeling, simulations, as described in the previous section has been used (e.g. using the Stella simulation package) with health professionals (e.g. doctors, nurses), health information technology professionals and healthcare managers. In addition, researchers have found that diagrams and visualizations of threat can be provided using a range of diagraming methods, such as use of Unified Modeling Language (UML) diagrams, data flow diagrams, swim lane diagrams and state diagrams. As well, open source tools such as TRIKE, an open source modeling tool (SourceForge.net, n.d.) and commercial tools such as ThreatModler, also used in modeling threats have appeared (MyAppSecurity, n.d.). These types of diagrams can be modfied and used for modeling threats due to hacking into systems (Coronado & Wong, 2014; Shostack, 2014) and they can be applied in modeling other risk areas such as technology-induced error. By systematically considering the health information technology data quality and integrity using the information technology risk framework in health care described in this paper (as shown in Fig. 1), the factors and parameters considered important for identifying

potential threat modeling can be used to educate health professionals about potential information technology risks. The target audience for use of these tools includes doctors, nurses, health information technology professionals, managers, privacy specialists and health information technology students at both undergraduate and graduate levels. Researchers are currently exploring the integration of threat modeling into the training of health professionals to educate them about the risks of a range of errors (from hacking to inadvertent technology-induced errors). The dynamic simulation approach to modelling allows trainees to explore a range of what-if scenarios where sources of error can be traced, modified and their impacts extrapolated by running simulation models (Borycki, Kushniruk, Anderson, & Anderson, 2010).

## 5. Discussion: Implications and further work

The implications of using the information technology risk framework in health care to train varying health professionals about risk are significant. The framework can be easily used in conjunction with simulations to guide the development of risk management competencies among doctors, nurses, health information technology professionals etc. Health professionals participate in simulations that are used for training about health information technology risks with the support of the framework. The framework helps health professionals to identify potential sources of error and risk experienced while taking part in the simulation exercises. The framework has helped educate health professionals to proactively identify how electronic patient data could be made inaccurate, modified and/or corrupted. In addition to this health professionals learn about the importance of maintaining data that is accurate, useful and free from corruption from any number of sources as well as the organizational strategies (e.g. Level 5 – Healthcare Data Quality and Assurance Policies; Level 2 – Monitoring Security and Accuracy of the Data) and information tools, techniques and activities (e.g. Level 6, Data Risk Management Strategies) that can be employed to ensure the accuracy, quality and safety of that data.

The framework is also being used to help guide development of new innovations for ensuring health data quality and integrity. For example, Kushniruk, Surich, and Borycki (2012) have presented on approaches to automatically detecting and classifying error in the transmission of healthcare data through networks (corresponding to interventions at Level 2 – the level of monitoring the accuracy of healthcare data. This has involved preliminary design of components to be added on top of standard network management and monitoring software to detect technology-induced errors and other types of data errors (Kushniruk, Surich, & Borycki, 2012). Much of this work is being based on ongoing empirical study of errors made in healthcare settings, leading to classification of errors in the development of an error ontology. Such an ontology can be used drive the automated detection of error patterns by providing a knowledge base of such errors. From our preliminary work, the researchers have found a number of error types in healthcare data transmission including: (a) data missing in transmission (b) ordering and format errors (c) destination errors (d) invalid data (e) message length errors (f) incomplete transmission (g) invalid or incorrect patient record numbers (h) routing errors (Kushniruk, Surich, & Borycki, 2012; Kushniruk & Borycki, 2015). Such work is necessary and is expected to lead to a knowledge base of error types and patterns that can be used to automatically detect if errors are being introduced and propagated in healthcare systems.

Future work in this area of research is taking place on several fronts. In one direction further work is refining health information technology data quality and integrity framework (see Fig. 1). Work will need to be done with experts in areas ranging from healthcare human factors, specialists in health information technology architecture, and

policy experts in the area of privacy and security of healthcare data. Work is also being done to extend the framework and educational approach to simulation modeling. This will include modeling a wider range of classes and types of healthcare data errors. Researchers are also working on basing the simulation and modeling outlined in this paper (as well as error detection components being designed) on a strong empirical basis from study of error in real and simulated healthcare settings and contexts. This work will be used to further drive the detection of error as well as form the basis of continued development of health professional training programs about information technology risk.

## 6. Conclusion

In summary, there are a number of possible educational implications of the work described in this paper. Firstly, there is a need for an improved understanding of the layers in the healthcare system, where error can occur and be detected, by health professionals. The framework described in this paper has been proven to be useful in educating health professionals about information technology risk. Health professionals who know where and how errors occur can help to develop targeted strategies for error mitigation and improve patient safety overall. Along these lines, the modeling and simulation of errors can lead to a better understanding of the implications and risks associated with letting an error propagate through a healthcare system. Finally, based on this type of work there is the potential to develop practical system components and training that will lead to identification of such errors by health professionals. Such an approach can be used to not only train health professionals but to help them identify potential data related issues. Here, health professionals are now able to alert organizations to errors that are propagating throughout the system. Thus, there are a number of aspects of educating health professionals about looking at healthcare data in a particular way, using the described framework, which will lead to overall improvements in patient safety.

## References

Borycki, E., & Kushniruk, A. (2005). Identifying and preventing technology-induced error using simulations: application of usability engineering techniques. *Healthcare quarterly (Toronto, Ont.), 8*, 99–105.

Borycki, E., Kushniruk, A., Anderson, J., & Anderson, M. (2010). Designing and integrating clinical and computer-based simulations in health informatics: From real-world to virtual reality. In S. Cakaj (Ed.). *Modeling Simulation and Optimization-Focus on Applications* (pp. 31–52). Vukovar: Croatia: InTech.

Borycki, E. M., Kushniruk, A. W., Bellwood, P., & Brender, J. (2012). Technology-induced errors: The current use of frameworks and models from the biomedical and life sciences literatures. *Methods of Information Medicine, 51*(2), 95–103.

Borycki, E. M., Kushniruk, A., Keay, E., Nicoll, J., Anderson, J., & Anderson, M. (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., Lemieux-Charles, L., Nagle, L., & Eysenbach, G. (2009). Evaluating the impact of hybrid electronic-paper environments upon novice nurse information seeking. *Methods of Information in Medicine, 48*(2), 137–143.

Bowman, S. (2013). Impact of electronic health record systems on information integrity: Quality and safety implications. *Perspectives in Health Information Management, 10*(Fall), 1c.

Coronado, A. J., & Wong, T. L. (2014). Healthcare cybersecurity risk management: Keys to an effective plan. *Biomedical Instrumentation & Technology: Cybersecurity In Healthcare*, *48*(s1), 26–30. doi: 10.2345/0899-8205.s1.26

International Ergonomics Association. (2015). *Definition and domains of ergonomics*. Retrieved from http://www.iea.cc/whats/

International Standards Organization (ISO). (n.d.). *ISO 31000 – Risk management*. Retrieved from http://www.iso.org/iso/home/standards/iso31000.htm

Institute of Medicine. (2011). *Health IT and patient safety: Building safer systems for better care*. Washington: National Academies of Science, Techology and Medicine.

Kushniruk, A. W., Bates, D. W., Bainbridge, M., Househ, M. S., & Borycki, E. M. (2013). National efforts to improve health information system safety in Canada, the United States of America and England. *International Journal of Medical Informatics, 82*(5), e149–e160.

Kushniruk, A. W., & Borycki, E. M. (2015). Development of a video coding scheme for analyzing the usability and usefulness of health information systems. *Studies in Health Technology and Informatics, 218*, 68–73.

Kushniruk, A. W., Borycki, E. M., Anderson, J. G., & Anderson, M. M. (2009). Preventing technology-induced errors in healthcare: The role of simulation. *Studies in Health Technology and Informatics, 143*, 273–276.

Kushniruk, A., Nohr, C., Jensen, S., & Borycki, E. M. (2013). From usability testing to clinical simulations: Bringing context into the design and evaluation of usable and safe health information technologies. *Yearbook of Medical Informatics, 8*(1), 78–85.

Kushniruk, A. W., Surich, J., & Borycki, E. M. (2012). Detecting and classifying technology-induced error in the transmission of healthcare data. In *Proceedings of 24th International Conference of the European Federation for Medical Informatics Quality of Life through Quality of Information*.

Kushniruk, A. W., Triola, M. M., Borycki, E. M., Stein, B., & Kannry, J. L. (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*, 519–526.

MyAppSecurity. (n.d.). *Enterprise threat modeling*. Retrieved from http://myappsecurity.com/threatmodeler-3-0-2/

Office of the Information and Privacy Commissioner for British Columbia. (2015). *Guide to access and privacy protection under FIPPA*. Retrieved from https://www.oipc.bc.ca/guidance-documents/1466

Ö hlund, S. E., Å strand, B., & Petersson, G. (2011). Interoperability in action-The case of electronic prescribing. In *Proceedings of the Fifteenth International Symposium for Health Information Management Research* (pp. 306–318). University of Zurich, Switzerland.

Perakslis, E. D. (2014). Cybersecurity in health care. *New England Journal of Medicine, 371*(5), 395–397.

Preece, J., Rogers, Y., Sharp, H., Benyon, D., Holland, S., & Carey, T. (1994). *Human-computer interaction*. Addison-Wesley Longman Ltd..

Sametinger, J., Rozenblit, J., Lysecky, R., & Ott, P. (2015). Security challenges for medical devices. *Communications of the ACM, 58*(4), 74–82.

Shostack, A. (2014). *Threat modeling: Designing for security*. John Wiley & Sons.

SourceForge.net. (n.d.). *Trike*. Retrieved from http://octotrike.org/

The Health Insurance Portability and Accountability Act (HIPPA). (1996). *Health information privacy*. U.S. Department of Health & Human Services. Retrieved from http://www.hhs.gov/ocr/privacy/hipaa/understanding/