DESIGNING A PROTOTYPE TO PROVIDE SECURE COMMUNICATION BETWEEN PHYSICIANS: A SURVEY TO EXAMINE ACCEPTABILITY AMONG USERS

DESIGNING A PROTOTYPE TO PROVIDE SECURE COMMUNICATION BETWEEN PHYSICIANS: A SURVEY TO EXAMINE ACCEPTABILITY AMONG USERS

A Thesis Submitted to the Graduate Studies in Partial Fulfillment of the Requirement for the

Degree of Master of Science, eHealth

M. Sc. eHealth Graduate Program
McMaster University
Ontario, Canada

By

Runki Basu

McMaster University | MASTER OF SCIENCE (2012)
Hamilton, Ontario | eHealth

TITLE: Designing a Prototype to Provide Secure Communication Between Physicians: A Survey to Examine Acceptability Among Users

AUTHOR: Runki Basu
B.Sc.(Hons) Economics, St. Xavier's College,
University of Calcutta
M.A. Economics, Jadavpur University

SUPERVISOR: Dr. Ann McKibbon

NUMBER OF PAGES: xii, 123

DISSERTATION COMMITTEE

Designing Prototype to Provide Secure Communication Between Physicians: A Survey to Examine Acceptability Among Users

By

Runki Basu

B.Sc. (Hons) Economics

M.A. Economics

DISSERTATION COMMITTEE

Supervisor:	Dr. Ann McKibbon Department of Clinical Epidemiology & Biostatistics *McMaster University*
Committee Member:	Dr. Tapas Mondal Department of Pediatrics *McMaster University*
Committee Member:	Dr. Norm Archer McMaster eBusiness Research Centre DeGroote School of Business *McMaster University*

ABSTRACT

OBJECTIVE: The aim of this study was to explore an alternative method of secure data exchange of patient information among physicians using their existing email.

METHODS: A four-step framework was designed to effectively conduct the research. It involved designing a prototype of a web-based system called ST-SecRx to simulate secure communication between physicians while exchanging sensitive patient data through email. The simulation achieved through the system was meant to determine and measure response of physicians to the use of secure email or similar communication tools for exchanging patient data. Physicians were invited to use ST-SecRx and subsequently participate in a survey to determine its acceptability and their perceptions about the usefulness of the software. Finally, the data collected from the survey were analyzed.

RESULTS: Data were collected from 22 physicians from various healthcare facilities in the province of Ontario, Canada. Eliminating questionnaires with no response resulted in 19 valid responses. Results revealed that 57.9% used email support provided by their organization for exchanging patient data. Over 70% acknowledged that factors such as: ease of use, not having to use an email different from the one provided by their employer, not having to create and remember new password every three to six months, and data transfer complying with privacy regulations would facilitate their use of ST-SecRx. More than 50% of the physicians felt that the simulated system as demonstrated to them was more secure and easier to use when compared to previously used methods of patient data

exchange through email. The majority of the physicians (from 57.9% to 73.7%) agreed with all the six questions on behavioral intention to use ST-SecRx. Overall 42% were willing to pay between $5 and $20 per month for ST-SecRx. Additional analysis of data by age, sex and discipline did not reveal any substantial differences in their enthusiasm to use the system.

CONCLUSION: The current research was successful providing data on what is important to clinicians who want to exchange data on patients with other clinicians. Use of systems similar to the prototype ST-SecRx could be an improvement over conventional email, provided that they would ensure security using encrypted technology under public key infrastructure methods and systems. Overall the physicians were satisfied with ST-SexRx and found it simple, fast, easy to use, and secure, and they indicated that they intended to use it if it were made available and it conformed to privacy and security standards. Also, such a secure system would have the potential to reduce the overall cost of healthcare by reducing duplication of diagnostic tests and making patient- specific information exchange faster. More research needs to be conducted with a larger sample size to validate the findings of this study. The limitations, dissatisfaction, and concerns expressed by the physicians who used ST-SecRx could direct future research. Future studies could include other healthcare professionals in the exchange of sensitive clinical data.

KEYWORDS: Secure Communication, Email Exchange, Physician-Physician Communication, Provider Communication, Internet Security

ACKNOWLEDGEMENTS

I would like to thank the following individuals:

Dr. Ann McKibbon: Dr. Ann Mckibbon has been my inspiration to continue on this journey of getting my Master's degree in eHealth. I have enormously benefited from her guidance as my mentor and guide for my Master's thesis. I thank her with all sincerity.

Dr. Norm Archer: Dr. Norm Archer has taught me valuable project management skills within the e-health realm. I thank him for being on the thesis committee and giving valuable help in completing my degree.

Dr. Tapas Mondal: I thank Dr. Tapas Mondal for giving me a real-world problem to consider. My thesis is a direct result of that problem. I thank him for his help and also for agreeing to be on my thesis committee.

Survey Participants:, My sincere thanks to all the physicians who took time to review the software and participate in the survey.

Dr. Samprasad Majumdar: I thank Dr. Samprasad Majumdar for helping me understand concepts of statistical analysis that helped me greatly in my thesis.

Iris Kehler: I thank Iris for being there for us whenever needed during this long journey of the M.Sc. e-Health program.

Bandana Basu: I thank my mother for all the support and encouragement I required to complete my Master's program.

Basudeb Mukherjee: Last but not the least, I thank my husband, Basu Mukherjee, to stand by me as I went through the Master's program.

Table of Contents

List of Figures

List of Tables

Glossary of Terms

EHR System	An Electronic Health Record system is a compilation of core health data managed and consulted by authorized health care providers and organizations, accessible by numerous authorized parties from a number of points of care, possibly even from different jurisdictions that conforms to nationally recognized interoperability standards.
EMR System	An Electronic Medical Record system is an electronic version of the paper record that physicians have traditionally maintained for their patients and which is typically only accessible by authorized clinician and their staffs within the facility or office that controls it. A “simple EMR,“ refers most often to an electronic record system created and maintained by a single physician in an office-based practice, must be distinguished from a “shared EMR” or “EHR”. In this document for US authors, who used the term EHR in their studies, we replaced EHR by EMR.
Encryption	The process of transforming information into a form that is unintelligible to those not possessing the required knowledge or authorization to decrypt it, such as a muddled stream of seemingly random symbols.
Health IT	Health Information Technology is the application of information processing involving both computer hardware and software that deals with the storage, retrieval, sharing, and use of health care information, data, and knowledge for communication and decision making.

List of Abbreviations

CAPTCHA	Completely Automated Public Turing test to tell Computers and Humans Apart
EHR	Electronic Health Record
EMR	Electronic Medical Record
GP	General Practitioner
HIPAA	Health Insurance and Portability and Accountability Act
HIT	Health IT
HTTPS	Hypertext Transfer Protocol Secure
IP	Internet Protocol
IT	Information Technology
PHIPA	Personal Health Information Protection Act (PHIPA)
PHR	Personal Health Record
PKI	Public Key Infrastructure
RDBMS	Relational Database Management System
REB	Research Ethics Board
ROI	Return on Investment
SCS	Standardized Communication System
SQL	Structured Query Language
SSL	Secure Socket Layer
TCP	Transmission Control Protocol
TLS	Transport Layer Security
URL	Uniform Resource Identifier
VPN	Virtual Private Network

1. INTRODUCTION

Canada is a leading nation in the world in terms of quality and access of care for its citizens. Today three major interconnected problems seem to exist in the current healthcare system: accessibility and security of patient data, quality of care, and cost of care (J. W. Hill & Powell, 2009). With a growing population of older people and increases in chronic illness, the speed with which the healthcare infrastructure is growing is falling short of its demand, posing a serious challenge to keeping Canadian people healthy or dealing with their health conditions as effectively as possible (J. W. Hill & Powell, 2009).

A major area of concern for the Canadian healthcare system has been lack of effective communication among healthcare providers, especially with respect to knowledge and data transfer and interoperability among different healthcare systems (Lang et al., 2006). In spite of healthcare being a technologically driven, data intense industry, many physicians still record patient information in a traditional manner by using paper based charts without taking full advantage of existing information technology (IT) systems (J. W. Hill & Powell, 2009)(Kaushal et al., 2005). Paper records are prone to errors and hence adoption of IT in healthcare is an effective way to enhance efficiency of flow of patient related information (Shortliffe, 2005).

With the advancements in IT, healthcare systems promise to improve quality of patient care, patient safety and security, lower healthcare costs, and reduce medical errors by facilitating interoperability among diverse healthcare systems across geographical

boundaries, reducing duplication of tests, creating public health awareness, and educating and training patients and healthcare providers on available healthcare information and technology (Chaudhry et al., 2006)(J. W. Hill, Langvardt, & Massey, 2007)(Walker et al., 2005)(Brailer, 2005)(Hillestad et al., 2005). Such advancements in the application of technology may make remote monitoring and accessing vital and accurate information and technology more efficient, and can also make knowledge-based and evidence-based information available to facilitate decision support (J. W. Hill & Powell, 2009)(Brailer, 2005).

During a patient's lifetime, the patient's medical record may be held by multiple healthcare providers using varied healthcare systems and kept in different data formats (Canada Health Infoway, 2011c)(Brailer, 2005). These providers could be from physician family health groups or teams, solo physician practices, hospitals, laboratories, pharmacies, chronic care facilities, walk-in-clinics, long-term and senior care facilities, hospices, rehabilitation centers, public health sites, and other points of care (Brailer, 2005). A patient's health information may also reside with government, health insurance providers, application providers for medical devices, employers and many other organizations or agencies (Appari & Johnson, 2010)(Mercuri, 2004). This flow and location of information is presented in Figure 1. Data in various clinical records of a patient accumulate over an extended period of time and include a great deal of personal information including identification, history of medical diagnoses, digital renderings of medical images, treatments, medication and dosing history, dietary habits, laboratory test results, presence of chronic diseases, allergies, adverse drug reactions, vaccinations,

surgeries, family history, sexual preference, genetic information, psychological profiles, employment history, income and physicians' subjective assessments of personality and mental state (Appari & Johnson, 2010)(Mercuri, 2004).

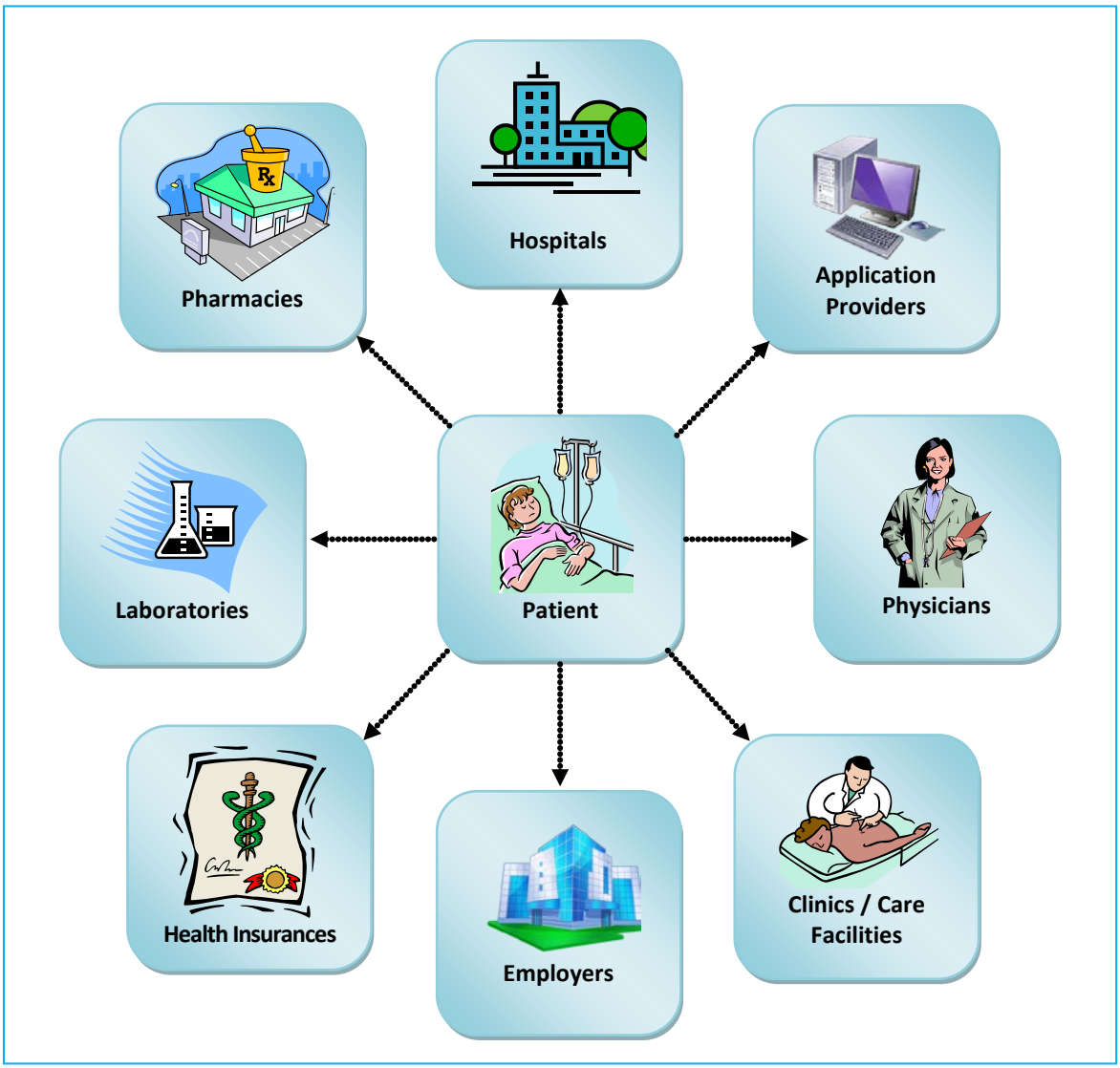


Figure adapted from Microsoft Health Vault Development Portal (Microsoft Health Vault, 2012)

Figure 1: Patient's Medical Records Held at Multiple Points

In addition to diagnosis and treatment, health records serve many other purposes (Appari & Johnson, 2010). Such purposes could be the use of information in developing

public health policies, enhancing efficiency of the system and clinical study of diseases (Hodge, December 2003) (Appari & Johnson, 2010). Public health officials and payers may have access to personal health data to process payments for services rendered (Appari & Johnson, 2010). Healthcare service providers can, in theory, use the records to optimize their operations and also share the records with regional health agencies to potentially improve quality of care (Appari & Johnson, 2010).

Patients often have the option of selecting their healthcare providers based on the providers' abilities, cultural orientation, proximity to a healthcare facility, or any other factor that is important to the patients (Brailer, 2005). In most cases, many of the systems the healthcare providers use currently store information in diverse proprietary formats (Appari & Johnson, 2010). These systems are not necessarily electronically connected and hence not interoperable to enable effective exchange of patient information (Canada Health Infoway, 2011c). Storing patient information in a variety of formats makes sharing information with providers difficult. A study by Walker et al. in 2005 concluded that in the US, implementing interoperability between diverse electronic medical records (EMR) systems and a health information exchange would likely save the healthcare industry $77 billion dollars annually (Walker et al., 2005). According to the study, implementation of EMR systems without the deployment of interoperability will lead to huge amounts of electronic data that cannot be shared outside the EMR (Appari & Johnson, 2010)(Walker et al., 2005)(Brailer, 2005). This in turn will emulate some of the same problems that exist with paper based records, especially the problems associated with proprietary

control by those who are creating the information (Appari & Johnson, 2010)(Walker et al., 2005)(Brailer, 2005).

Access to accurate information and its associated technology wherever and whenever it is needed plays a key role in effective management of patient care. Physicians commonly need to treat patients even in the absence of information about the patient's medication history, or any specific health conditions the patient may have. Such practice without adequate information may lead to serious complications including drug-drug interactions, drug allergies and drug overdoses (Moya, 2011). In many instances physicians, due to lack of coordination, are unaware of tests ordered by other healthcare providers, thus repeat tests which may increase the healthcare costs to the economy (Moya, 2011)(Brailer, 2005).

The most effective way to resolve the communication issues described above is implementation of a network of different but interoperable HIT systems to enhance storage, retrieval and portability of electronic patient information among these diverse healthcare systems (Brailer, 2005)(Ministry of Health British Columbia, 2012a)(Canada Health Infoway, 2012). Such HIT systems, when implemented will allow seamless portability of patient data transfer between varied healthcare systems such as electronic health record (EHR) systems, computerized provider order entry systems, pharmacy information systems, laboratory systems, radiology systems, clinical decision support systems, practice management systems, financial systems, administrative systems, hospital information management systems and many more systems used by healthcare providers (Canada Health Infoway, 2011b)(Canada Health Infoway, 2011c).

While the terms EMR and EHR systems are used interchangeably in the literature, for this document we used the terms as they are used in Canada. In essence, we use the term EMR system to imply an electronic record keeping system where medical record of patients are created and maintained by a single physician in an office-based practice. And we use the term EHR system to refer to interoperable systems meant for use in larger setups like hospitals where information can be created, shared, exchanged, managed, retrieved, stored and processed accurately and seamlessly among authorized healthcare providers while maintaining privacy, confidentiality and security and conforming to certain accepted standards, guidelines, policies, legislations and methodologies (Ministry of Health British Columbia, 2012a) (McKibbon et al., 2011) (Grogan, 2006) (Ministry of Health British Columbia, 2012b)(Canada Health Infoway, 2012).

In should be noted that, in the US, the terms EMR and EHR both imply electronic medical information keeping systems that physicians have traditionally maintained for their patients and which are typically only accessible by authorized clinicians and their staffs within the facility or office that controls it. In this document, for US authors who used the term EHR in their studies, we replaced EHR by EMR.

In addition to EMR systems, data from personal health record (PHR) systems and self-monitoring HIT devices including mobile HIT systems can potentially help both patients and providers to work in collaboration for better management of health even in remote locations (Brailer, 2005) (Ministry of Health British Columbia, 2012a). The HIT system will enable authorized clinicians and other healthcare providers to have full access

to longitudinal medical records about their patients (Ministry of Health British Columbia, 2012b)(Ministry of Health British Columbia, 2012a)(Canada Health Infoway, 2012). Patients would likely be more informed about their medical conditions and could move freely between different physicians and other healthcare providers without losing information (Brailer, 2005). Interoperability could enable real-time streaming of video interactions among physicians and their patients (Brailer, 2005). With use of all of these HIT resources fewer errors and less duplication of tests will likely happen (Hillestad et al., 2005). Furthermore, within a controlled environment of an EHR system, it is easier to implement and to maintain regulations relevant to security, privacy and portability of patient data across the healthcare continuum (The Canadian Medical Protective Association, 2012) .

In Canada, in an effort to provide a solution to these growing problems of great concern, the country's First Ministers formed Canada Health Infoway in 2001. It is a not-for-profit corporation funded by the Government of Canada. Canada Health Infoway is working with the nation's ten provinces and three territories to deploy a network of different HIT systems that will comply with their Electronic Health Record Solution (EHRS) Blueprint (Canada Health Infoway, 2012). The EHRS Blueprint, an information systems architecture, provides a technology framework that permits sharing of patient health information between authorized healthcare services providers across Canada.(Canada Health Infoway, 2012) Its aim is to accomplish successful implementation of certain specific HIT systems as trials in one province and subsequent replication in other regions (Canada Health Infoway, 2011a). According to Canada Health

Infoway, once implemented, such HIT systems will allow multiple healthcare providers to access clinical information captured by other healthcare providers for the same patient at the point of care (Canada Health Infoway, 2012).

This implementation could thereby provide Canadians across the nation with a better healthcare system (Canada Health Infoway, 2011b). Development and implementation of HIT systems following the EHR Blueprint of Canada Health Infoway from coast to coast is a multi-billion dollar investment which has the potential to establish a strong and efficient healthcare system (Lang et al., 2006)(Moya, 2011)(Canada Health Infoway, 2011d)(Canada Health Infoway, 2012). This implementation will become an integral part of health care delivery in Canada and will likely facilitate patient care by improving the flow of information and portability of medical records across diverse healthcare platforms, thus allowing the healthcare providers better access to patient information as, and when, needed (Lang et al., 2006)(Moya, 2011)(Canada Health Infoway, 2011d)(The Canadian Medical Protective Association, 2012).

According to Canada Health Infoway, once this monumental task of implementing HIT systems compliant with their EHRS Blueprint is accomplished, authorized healthcare providers across the country will have access to a secured comprehensive EMR of a patient which they can share and exchange (Canada Health Infoway, 2011b)(Canada Health Infoway, 2011c)(Canada Health Infoway, 2012). The benefits of such HIT systems are manifolds and are described below.

Enhanced Quality of Patient Care & Patient Safety: Enhanced Quality of Patient Care & Patient Safety: Potential benefits of an interoperable HIT system could

be reduced wait-time, faster treatment, enhanced accessibility of healthcare even to those living in remote locations and those with limited or no mobility, easier remote monitoring, self management and improved patient safety from adverse drug interactions, allergies or misinterpretation (Chaudhry et al., 2006)(Hillestad et al., 2005)(Shekelle, Morton, & Keeler, 2006)(The Canadian Medical Protective Association, 2012).

Interoperability of Systems & Portability of Information: Another benefit of interoperable HIT systems could be faster decision making once medical records become available to healthcare providers across diverse systems. The physical presence of a patient or direct data collection may not always be required. Interoperability can lead to increased efficiency in business and administrative processes across the healthcare continuum.(Brailer, 2005)(J. W. Hill & Powell, 2009)

Lower Healthcare Cost: Portability of information helps reduce duplicate record keeping and unnecessary duplicate tests thus likely lowering costs, optimizing resources, making healthcare more affordable and increasing the return on investment (ROI).(Walker et al., 2005)(J. W. Hill & Powell, 2009) (Hillestad et al., 2005)(Shekelle et al., 2006)(The Canadian Medical Protective Association, 2012)

Accessibility to Evidence-based & Knowledge-based Information: Interoperable HIT systems are expected to improve decision support and improve healthcare delivery (Nieuwlaat et al., 2011) (Shiffman, Liaw, Brandt, & Corb, 1999)(The Canadian Medical Protective Association, 2012).

Despite the multiple benefits of interoperable HIT systems, their implementation is still very slow and is at a very primitive stage (J. W. Hill et al., 2007)(DePhillips,

2007). Several barriers as well as diverse opinions exist about successful implementation of interoperable HIT systems. Some of the major impediments towards adoption of interoperable HIT systems can be attributed to massive implementation costs, disruptive effects on practices, selection of the appropriate system, and slow and uncertain financial ROI (Hillestad et al., 2005)(DePhillips, 2007).

Globally, there is a trend to implement HIT solutions with an aim to improve and enhance the quality and safety of healthcare, even though these systems are costly (Black et al., 2011). Black *et al.* conducted a systematic review of systematic reviews to measure the efficiency of several HIT systems on quality and safety of care. According to the analysis little evidence validates the benefits claimed by policy makers about these technologies. The finding seems to reflect a serious lack of effective research on the risks associated in implementing such technologies and their supposed cost advantages (Black et al., 2011).

A systematic review by Chaudhry *et al.* analyzing the effect of HIT on quality, efficiency and cost of healthcare revealed three key benefits on quality: "increased adherence to guideline-based care, enhanced surveillance and monitoring, and decreased medication errors" (Chaudhry et al., 2006). According to their review, EHR systems and computerized provider order entry systems (CPOE) usually had decision support functionalities embedded in them. However, no major evidence was available on how effective multifunctional commercially developed systems were (Chaudhry et al., 2006). Use of consumer health technology such as PHR systems and also advanced topics like interoperability were not much supported by evidence found in this systematic review

(Chaudhry et al., 2006). Major improvements were observed in primary and secondary preventive health and reduced utilization of care by offering point-of-care decision support through CPOE (Chaudhry et al., 2006). Such decision support included automated calculation of pretest probabilities of diagnostic tests, showing previous laboratory and radiology test results and costs, and provision of computer alerts. With help from point-of-care decision support, the clinicians may have determined and made less number of service utilization requests and that may have caused the decrease in service utilization (Chaudhry et al., 2006). However, it was not evident from the study whether HIT can improve quality and efficiency of healthcare delivery (Chaudhry et al., 2006). Unless the stakeholders are better informed about the benefits expected from adoption of HIT with respect to technology improvement and ROI, deployment of HIT would remain a challenge for the stakeholders (Chaudhry et al., 2006).

Developing efficient interoperable EMR or EHR systems integrated with multiple HIT systems still remains a challenge for policy makers, clinicians and other healthcare providers, healthcare information technologists, and advocates of EHR and EMR system adoption. Successful implementations of such HIT systems are expected to facilitate data accessibility and resolve interoperability issues. However, major concerns for adoption of interoperable EMR or EHR system seem to be privacy and security of patient information. Implementation and execution of appropriate regulations and standards required for such HIT system implementation is another concern for decision makers (Appari & Johnson, 2010).

Even though the barriers described here are universal among healthcare systems internationally, it must be recognized that each nation's healthcare system faces its own unique challenges that may or may not be relevant to other nations (DePhillips, 2007).

Until interoperable HIT systems are implemented across the nation, exchanging patient information in a secure and efficient way remains a challenge among healthcare providers. Implementation of a network of diverse HIT systems compliant with Infoway's EHRS Blueprint across geographical boundaries is expected to resolve or reduce interoperability issues among diverse healthcare systems (Canada Health Infoway, 2012). Exchanging patient information between healthcare providers, especially clinicians within and outside of a healthcare organization can be a time-consuming process that sometimes affects workflow and delays patient care for diagnosis and treatment and can result in duplication of tests (Walker et al., 2005)(Brailer, 2005).

A common practice with healthcare providers is to send important patient information and sensitive medical data through email. Since the first email sent by Ray Tomlinson in 1971, email over the following decades, has gained immense popularity (Car & Sheikh, 2004a). Extensive public use of email began during the early 1990s and has become a part of our daily routine (Car & Sheikh, 2004a). Over the years use of email has grown exponentially because it is easy to use, fast, and an efficient means of communication (Car & Sheikh, 2004a). Email can be sent and received anytime using a computer, laptop, smart phone, or a tablet (Car & Sheikh, 2004a). Physicians can use email to consult and collaborate with multiple colleagues simultaneously (Car & Sheikh, 2004a). Sending patient information by email also minimizes errors associated with hand

written notes. However, physicians should be aware of potential risks and the ramifications of using email for exchanging patient information and the need to safeguard the privacy and confidentially of such information (Car & Sheikh, 2004b)(Car & Sheikh, 2004a). Professional protocols, ethical considerations, and healthcare laws and guidelines that are applicable to traditional communication should also be applied to email communication (Car & Sheikh, 2004b)(Car & Sheikh, 2004a)(Anderson, 1996).

While email use has the ability to facilitate improved healthcare delivery, sharing patient health records via email raises grave concerns among physicians, patients, healthcare providers and privacy advocates about privacy and confidentiality of personal medical information of a patient (Car & Sheikh, 2004a)(Car & Sheikh, 2004b)(Baker, Wagner, Singer, & Bundorf, 2003). All of these stakeholders are apprehensive about unauthorized interception of unencrypted email and receipt or retrieval of emails containing patient medical records by unauthorized people such as hackers or intruders (Car & Sheikh, 2004a).

Evidence from research suggests that breaches of security of patient health information have happened due to lack of proper implementation of adequate security protection (Appari & Johnson, 2010). Use of email in the healthcare industry has grown without adequate infrastructure to deal with security problems (Car & Sheikh, 2004b).Without implementing appropriate encryption technology, security of unencrypted email may inadvertently lead to serious breaches of privacy and confidentiality of patient information (Car & Sheikh, 2004b). Failure to implement appropriate security legislation, policies, regulations and standards have resulted in

patients becoming victims of financial loss or social disgrace and suffering from traumatic psychological agony (Appari & Johnson, 2010).

The Department of Pediatrics at McMaster Children's Hospital has been experiencing problems exchanging patient information outside the organization. Often, the physicians at McMaster Children's Hospital refer patients to outside care facilities, particularly to the Hospital for Sick Children in Toronto. In the past, physicians have commonly sent relevant patient data to attending physicians at other hospitals through the email service provided by McMaster University. This practice has been stopped at McMaster Children's Hospital after having been flagged by a privacy audit as a violation of patient privacy.

This thesis endeavors to address the security issues involved in sending patient data by email and to develop a solution that can provide secure communication among clinicians that complies with privacy regulations.

1.1. Background and Related Work

Communication between clinicians within and outside healthcare organizations, with regards to patient health information, has always been a challenge. Communication interruptions can disrupt workflow and may affect the diagnosis and treatment of a patient. Patients interact with a variety of healthcare providers such as physicians, nurses, pharmacists. Additionally, these healthcare providers must collaborate, communicate and exchange clinical information effectively using methods that are cost-effective and secure. Email can be an efficient, time-saving and cost-effective means for delivery of

healthcare-related information. However, little has been published about the use of email by clinicians to communicate with other clinicians or healthcare providers for sharing and exchanging patient health information (Car & Sheikh, 2004a). The overwhelming majority of literature is on the use of electronic communication for patient-physician communication or patient-provider communication. A possible cause for the modest amount of published information on clinician-clinician electronic communication could be the limited adoption of email by healthcare providers to exchange sensitive patient health data. Undoubtedly, clinicians lack confidence in the security of email as a mode of transmission of electronic patient information and are apprehensive in using email as a method of transmission for patient health data (Baker et al., 2003). Email exchange servers traditionally used in hospitals or clinics generally do not provide secure encrypted exchange of information (Car & Sheikh, 2004a)(Car & Sheikh, 2004b). Standard email systems lack adequate security to comply with privacy, security, and confidentiality and fail to conform to health-specific privacy legislation like the Personal Health Information Protection Act (PHIPA) in Ontario, Canada (Hsiao et al., 2011).

Secure exchange communication through virtual private network (VPN) connections, web-messaging solutions, and encrypted email communication between healthcare providers are available commercially. However, little published literature addresses the efficacy of those solutions.

A report by Evans *et al*. (2001), surveyed both general practitioners (GPs) and hospital physicians in West Midlands, UK on their use of email (Evans et al., 2001). The survey involved 224 questionnaires sent to physicians at three large hospitals and to 300

GPs selected randomly from a list of 711 (Evans et al., 2001). Overall response rate was 60%. Generally speaking, 65% of the 314 respondents used email, and among them, 84% of hospital physicians used email compared with 55% of GPs (Evans et al., 2001). Email was primarily used as a tool for communication with friends and family (92%) and colleagues (61%)(Evans et al., 2001). Only 7% used email for transmitting clinical data and a smaller percentage (3%) used it for sending and receiving referrals (Evans et al., 2001).

Age appeared to have played a significant role in email usage, with usage being the highest in the 20–29-year age group and lowest among the 60 plus age group (Evans et al., 2001). The majority of the respondents (60%) believed that, for transmission of patient data, email was neither a secure nor a confidential communication tool (Evans et al., 2001). Although email was often used by the survey respondents for social communication, the use of email in work by clinicians was low (Evans et al., 2001). Nonetheless, 90% of the participants believed that in five years their use of email in their work would increase significantly (Evans et al., 2001).

Electronic exchange of information with reference to imaging data between offsite and onsite physicians is a vital component of patient care (Arnold, Bui, Morioka, El-Saden, & Kangarloo, 2007). Arnold et al. (2007) summarized the development of a prototype web-based reporting system with a feedback loop for onsite-offsite clinician communication of radiologic images (Arnold et al., 2007). The article dealt with an open-source, distributed image referral and communication system among the clinicians. The system provided a web-based input feedback mechanism that would collect data relevant

to the images and gather responses from radiologists and then return information back to the referring clinician (Arnold et al., 2007). This prototype web-based reporting system designed for the study has the potential of being adopted and customized for any onsite and offsite clinician communication loop (Arnold et al., 2007).

Implementation of an electronic information exchange system in healthcare is expected to improve workflow, increase efficiency, and reduce resource utilization such as repeat visits to emergency department, admissions to hospital, mean length of stay, duplication of laboratory tests and imaging and other expensive medical resources (Lang et al., 2006). However, a study conducted at an adult teaching hospital in Montreal in 2002 revealed no apparent benefit of their electronic information exchange system with respect to reductions in resource utilization (Lang et al., 2006). Lang *et al.* developed a web-based standardized communication system that allowed GPs to receive comprehensive emergency department reports of their patients (Lang et al., 2006). A randomized controlled trial revealed that an electronic transfer of information between emergency department and family physicians did not result in a significant reduction in resource utilization in either of the two care facilities studied (Lang et al., 2006). Failure to yield any positive outcome may be due to limitations of the study. The physicians may have overstated their lack of access to information, as the study did not reveal any reduction in duplication of tests by physicians having access to the information. The existing practice of using carbon copies of emergency department notes to share information with physicians may have negatively impacted the outcome of both the use of

the standardized communication system intervention and the use of resource utilization (Lang et al., 2006).

Articles have reported success stories of HIT implementation in European countries whereby physicians and other healthcare providers are able to exchange patient information electronically through nationally connected networks. Denmark is at the forefront of network communication and is one of the world's leading countries to have been able to implement a national health network successfully (Protti & Johansen, 2010). According to J Michael Hasenkam, chairman of the Danish Medical Associations (an umbrella organization for all 170 medical-scientific societies in the country), the Danish success is dependent on two factors. First, their records are held within a range of databases of different types that are available via the national health portal. Second, each and every individual in country can be tracked down by a national recording system. This system records and synchronizes each patient's encounter with the healthcare system such that it can be traced down to the basic prescription level (The Economist Intelligence Unit, 2012).

Protti and Johansen (2010) observed that in Denmark almost all primary care physicians act as healthcare gatekeepers, and use one of many interoperable EMR systems. Most of these systems have advanced clinical functionality (Protti & Johansen, 2010)(The Economist Intelligence Unit, 2012). These EMR systems are connected to the national health network, facilitating interoperability between different systems and allowing electronic exchange of clinical data amongst specialists, hospitals, pharmacies and other healthcare providers (Protti & Johansen, 2010). In the primary care sector, it

has been observed that most clinical communications are electronically exchanged over the country's national health network (Protti & Johansen, 2010). EMR systems in Denmark, in addition to allowing physicians to record patient information and notes, act as a central repository for information coming from outside their offices through their national network (The Economist Intelligence Unit, 2012). Denmark also has regional databases for patient hospital records and national databases for medication. Both primary care and hospital-based physicians have access to these databases. Patients have limited access to view data from EMR systems and hospital records through the national portal and Denmark's citizen's portal (The Economist Intelligence Unit, 2012). Use of EMRs by primary care physicians has reduced paperwork, saved time, and allowed them to see 10% more patients (The Economist Intelligence Unit, 2012). The EMR systems have also enhanced quality of care by triggering automated reminder and alerts for drug-drug interactions (The Economist Intelligence Unit, 2012).

The Danish success story provides a model from which lessons can be learnt about challenges, obstacles, achievements and factors that contributed towards success in electronic communication of patient data (Protti & Johansen, 2010). While it was not until 2004 that primary care physicians were mandated to use HIT, Danish national policies dating back to early 1990s, peer pressure, and the use of a national health system integrator (MedCom) contributed towards successful implementation of EMRs. These policies included developing national standards for interoperability of electronic data, incentivizing primary care physicians financially for phone and email consultations and creating a method by which physicians who used EMR systems were reimbursed quickly.

System integration and interoperability could be achieved seamlessly because MedCom was used to develop a national HIT infrastructure and thereby set standards for electronic communications and information. Primary care physicians were able to communicate thorough MedCom with other healthcare providers using a clinical messaging system (Protti & Johansen, 2010).

A Dutch study by Branger *et al*. evaluated the effects of the introduction of electronic data interchange between primary and secondary care providers involving three types of messages: admission-discharge reports from hospitals to GPs; laboratory reports from hospitals to GPs and free text messages among GPs. The majority of the GPs reported that electronic communication provided accurate, faster and complete access to patients' medical information, and also reduced their workload (Branger et al., 1992).

Although the literature is sparse and little evidence exists on use of electronic communication as a tool for healthcare provider-provider transmission of patient health information, some studies reveal the use of email and web messaging services was an effective means for patient-clinician communication.

With advancements in technology, Internet applications for communication, especially email, have become an important and more convenient tool for patient communication over the traditional methods of face-to-face and telephone consultation (Ye, Rust, Fry-Johnson, & Strothers, 2010). A systematic review by Ye *et al.* (2010) on the use of email in patient-provider communication revealed that email may improve communication between patient and providers thereby enhancing the quality of patient care (Ye et al., 2010). While benefits and convenience of using email were recognized by

both patients and providers, concerns were expressed by both the groups over the privacy, confidentiality and security of such email because of the nature of information transmitted (Ye et al., 2010).

Whenever health information is requested by any individual it is the responsibility of the healthcare provider to ensure, before releasing any information, that the individual has the legitimate right to access such information (Gerstle, 2004). Physicians have ethical and legal responsibility to protect the privacy and confidentially of patient information including their communication with patients. Email is considered to be a convenient and efficient means of patient-provider communication, but it lacks adequate security to comply with standard healthcare guidelines such as PHIPA in Ontario, Canada (Hsiao et al., 2011). Emails exchanged over the Internet are generally not encrypted and may inadvertently expose sensitive details about patients' medical information (Gerstle, 2004) (Mandl, Kohane, & Brandt, 1998). Unencrypted messages also have the risk of being intercepted by a potential unauthorized person who then can access to confidential patient information in the email (Gerstle, 2004) (Car & Sheikh, 2004a). The evolution of the Internet is witnessing more and more organized and targeted attacks. More of these attacks are attempts of identity theft. Such threats include Trojans, spams, spyware, phishing, and other malware (Keshavjee, Pairaudeau, & Bhanji, 2006). With the wide spread adoption of Internet technology, the medical profession is becoming increasingly vulnerable to such high-tech threats (Keshavjee et al., 2006). Typically, computer installations are secured by firewalls and virus checkers. Such technologies have their limitations in protecting the computers that they are designed to protect (Keshavjee et al.,

2006). Any system designed to protect medical installations or clinicians' offices need to carefully consider such limitations and promote pro-active monitoring of such installations of such installations (Keshavjee et al., 2006). Developing a secure server for electronic communication may reduce such risks but has its own deficiencies.

Hsiao *et al.* (2011) evaluated the impact of a secure web messaging system implemented for a pediatric subspecialty outpatient, academic respiratory clinic in New Haven, Connecticut (Hsiao et al., 2011). The system allowed secure, encrypted, firewall protected, and HIPAA compliant electronic communication (Hsiao et al., 2011). One hundred and twenty-seven patients or their families who had previously used the Internet were surveyed. Only 5 messages were sent by patients in the 8 months following the implementation (Hsiao et al., 2011). Web messaging was found to be too technically complex to use and lacked personal touch. According to Hsaio, using the telephone was more convenient for patients and 2363 telephone calls were made during the same time period (Hsiao et al., 2011).

A study by Kittler *et al.* found that the reasons for physicians being resistant towards using a web-based portal for electronic communication with their patients is their concern about security of transmission of patient health information over the Internet, lack of compensation and increased workload (Kittler et al., 2004).

In a study in the Netherlands, Branger *et al.* observed that it is crucial for healthcare providers to communicate and exchange information when one patient is jointly treated by more than one physician (Branger, Van't Hooft, & Van der Wouden, 1995). In such circumstances it is important to have integration of records from multiple

sources (Branger et al., 1995). The researchers developed a new message, called MEDEUR to integrate patient data exchange between computer-based patient records. EMR systems were used by both GPs and specialists to store medical data of jointly treated patients. Physicians used the MEDEUR message standard to communicate with other physicians and healthcare providers. The use of an electronic data exchange system enabled electronic transmission of patient health data from a physician's to another physician's computer system thus avoiding the task of retyping the information (Branger et al., 1995).

It is important to note that such systems as described above were successful and could operate only because of integration of interoperable EMR systems, which allowed portability of medical information. Achieving secure communication within an integrated system of EMRs is not an easy task, especially for complex healthcare systems such as those in the US and Canada which has many healthcare providers who use multiple cumbersome systems that are not interoperable.

eHealth Ontario, an independent agency of the Ontario Ministry of Health and Long-Term Care in Canada, spent approximately $16 million to build an email service system for healthcare providers called ONE® Mail to share patient health information quickly and securely among registered users (Office of Auditor General of Ontario, 2009) (eHealth Ontario, 2012). Currently, ONE® Mail is used across the province of Ontario by pharmacies, hospitals, long term care facilities, drug addiction, substance abuse and mental health clinics, various community healthcare centers, and other points of care. ONE® Mail has solutions for both smaller and larger healthcare organizations (eHealth

Ontario, 2012). ONE® Mail Direct, designed for smaller organizations such as individual practices or clinics, is a comprehensive email service hosted in eHealth Ontario's secured environment. ONE® Mail Direct requires participating healthcare organizations to have e-mail accounts with ONE® Mail, thus allowing subscribers to securely exchange email messages that include patient health records with any registered users from other participating organizations (eHealth Ontario, 2012). ONE® Mail Partnered on the other hand is designed for larger organizations such as hospitals and allows subscribers to use their existing email systems to exchange patient health information with subscribers from other participating organizations (eHealth Ontario, 2012).

However, ONE® Mail has been a major disappointment for healthcare providers in Ontario and has been criticized by healthcare providers and also by the Office of the Auditor General of Ontario (Office of Auditor General of Ontario, 2009) (Keshavjee, 2010) (Webster, 2012).

A special report by the Office of the Auditor General of Ontario stated that in 2006 two-thirds of ONE® Mail accounts were inactive (Office of Auditor General of Ontario, 2009). The report also revealed that, in a separate survey, 53% users of ONE Mail expressed dissatisfaction with ONE® Mail (Office of Auditor General of Ontario, 2009). An internal evaluation is supposed to have determined that ONE® Mail to be inferior to commercially available products (Office of Auditor General of Ontario, 2009)(Webster, 2012). The evaluation further found that ONE® Mail's dependence on the SSHA (Smart System for Health Agency) network actually hampered its performance as well as increasing its outage rate (Office of Auditor General of Ontario, 2009).

According to Dr. Karim Keshavjee, a primary care health informatician and clinical architect with over 20 years of experience in EMR/EHR implementation, the low rate of adoption of ONE® Mail could be because of its serious usability issues. While using ONE® Mail he found that the password was required to be changed every six weeks. However, this requirement was later changed to 90 days on Dr. Keshavjee's recommendation. Another problem with ONE® Mail he noted at the time was that, while changing a password one could not use any previous passwords created for the ONE® Mail system. It had to be a completely new password never used before with ONE® Mail. While this business rule for the password was built into the system as a security feature, it added to the inconvenience of using the system. Dr. Keshavjiee comments "eHealth Ontario has the most secure e-mail facility in the world. It is so secure, that even providers can't get in!" (Keshavjee, 2010). He also pointed out that ONE® Mail has not been popular with healthcare providers because of eHealth Ontario's inability to understand end-user requirements and their lack of "value-driven focus" towards achieving "ease of use" (Keshavjee, 2010). When eHealth Ontario procures eHealth technologies without understanding the unique needs of the healthcare providers it leads to "one size fits all" technologies designed to satisfy everyone but actually satisfies none (Keshavjee, 2010). A common practice in the healthcare sector is to blame the clinicians for their resistance to accept new technology when a product or a service does not meet the requirements of the clinicians (Keshavjee, 2010).

The literature discussed in the previous sections demonstrates that attempts have been made to provide healthcare providers with a secure data exchange solution with

potential to improve quality of patient care. However, the way these systems were designed, developed and implemented resulted in limited acceptability among users and did not accomplish the expected improvements.

Thus, additional research in providing a secure data exchange solution among healthcare providers is required to ensure successful acceptance of these technologies among healthcare providers and to hopefully improve patient care.

1.2. Research Question

The goal of this study is to design a web-based system to simulate secure communication between physicians while exchanging sensitive patient data through email, and to examine this tool's acceptability among users and their perceptions of its usefulness.

The majority of the research conducted so far is on systems that allowed patient information exchange between clinicians and patients. A few journal articles discuss secure data exchange between healthcare providers. Unrestricted transfer of patient data through email is a clear violation of the patients' privacy and security. Thus the aims of this study were to:

- Explore an alternative method of secure data exchange of patient information among physicians using their existing email.
- Simplify the process of sending patient data in a secure way.
- Review the response of physicians regarding the use of such a method of data exchange.

2. METHODS

The purpose of this research was to design and develop a prototype of a web-based system to simulate secure communication between healthcare providers while exchanging sensitive patient data through email. The customized data presentation on the web was built to simulate secure patient data against privacy violation. The simulation achieved through the system was meant to determine and measure the response of physicians while trying to use secure email or similar communication tools for exchanging patient data. After the system was developed, tested, and running free of any errors, physicians were invited to use the system. Subsequently a survey was conducted to examine acceptability and other perceptions of the system among physicians after they had used the prototype.

While designing the prototype the aim was keep the system simple, stable, and easy to use so that it could be used efficiently by even the most technologically unskilled healthcare providers. The prototype was built, keeping in mind that an ideal system does not require healthcare providers to change their workflow in any substantial way nor does it require them to use and remember new email addresses, passwords, or website URLs. The prototype was developed in a way that it could reside inconspicuously within an existing IT infrastructure without requiring any major additional resource allocation and would allow the healthcare providers to use their existing email systems to communicate with each other. The prototype had another desirable feature, in that it did not require any added hardware.

The objective was to offer clinicians at McMaster Children's Hospital the ability to communicate and exchange patient data with their colleagues outside their hospital facility without violating patient privacy. Current communication options available at McMaster Children's Hospital do not allow the use of email and the Internet to share patient data as well as clinical notes of physicians. Sending information by courier or Canada Post is cumbersome, time-consuming, and expensive, and Ontario's Information and Privacy Commissioner has ordered Cancer Care Ontario to stop transferring reports containing patient information to physicians in paper format (Canadian Healthcare Technology, 2012). It is thus increasingly becoming necessary to consider the use of technological solutions that ensure privacy, security and confidentiality for transferring patient health information (Canadian Healthcare Technology, 2012).

To effectively conduct this research, a four-step framework was designed. The framework involved designing a prototype of a web-based system to simulate secure communication between healthcare providers while exchanging simulated sensitive patient data through email. The web-based prototype developed was called ST-SecRx. Subsequently, physicians were invited to use the online prototype ST-SecRx. The physicians who used ST-SecRx were asked to participate in a survey to assess the acceptability of the tool and to provide their perceptions about the usefulness of the software. Finally, the data collected from the survey were analyzed.

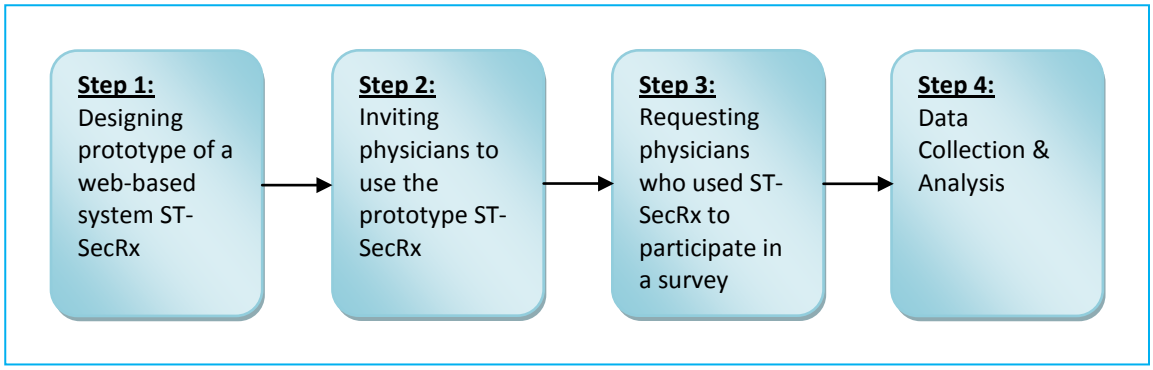


Figure 2: Study Framework

2.1 Designing the Prototype

The prototype design does not require transmission of any patient data directly through email. The prototype of the web-based system ST-SecRx involves storing dummy patient data in a database in the server. The system generates a hyperlink and username and password for the recipient physician. During any real deployment of a similar system, this hyperlink will be encrypted using commercially available state of the art encryption technology. It should be noted that at the time of generating the username and password we used CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) to protect the users and to enhance the security of the ST-SecRx.

Computer scientists Luis von Ahn, Manuel Blum, Nicholas Hopper and John Langford, working at the Carnegie Mellon University created a web security tool and coined the term CAPTCHA, which is a computer software system that is capable of cognitive responses that can only be passed by humans under the current available

technologies (Carnegie Mellon CyLab Portal, 2012)(reCAPTCHA, 2012). CAPTCHA uses simple math tests to prevent automated software from performing actions that might mimic those of a human user. This is commonly used for user-authentication by computer systems to ensure that a response to the system is actually initiated by humans, and is not actually a response that is auto-generated by another non-human computer system (Carnegie Mellon CyLab Portal, 2012)(reCAPTCHA, 2012). CAPTCHA has multiple applications that include, but are not confined to, SPAM prevention, protecting online polling against automated and fraudulent polling, protection of online registration, preventing search engine bots from indexing web pages, by requiring password systems to enter a CAPTCHA after a certain number of unsuccessful logins (Carnegie Mellon CyLab Portal, 2012)(reCAPTCHA, 2012).

Once the ST-SecTx generates the hyperlink and the username and password, the system sends the hyperlink along with the username to the recipient physicians by an email. The ST-SecRx sends a second email for transmitting the password. The reason behind sending username and password by separate mails is to enhance security. The data can be reviewed by the target physicians by clicking on a hyperlink. The clinicians at McMaster Children's Hospital or any other hospital, clinic or healthcare facility can share (i.e., send) the hyperlink with the target physicians. The hyperlink does not carry any identifier that can be linked to a specific patient. In an actual implementation, the system will integrate with Public Key Infrastructure (PKI) to ensure safety and security of patient data (Adams & Lloyd, 2002). The system architecture and the workflow of ST-SecRx have been presented in Figure 3, 4, and 5.

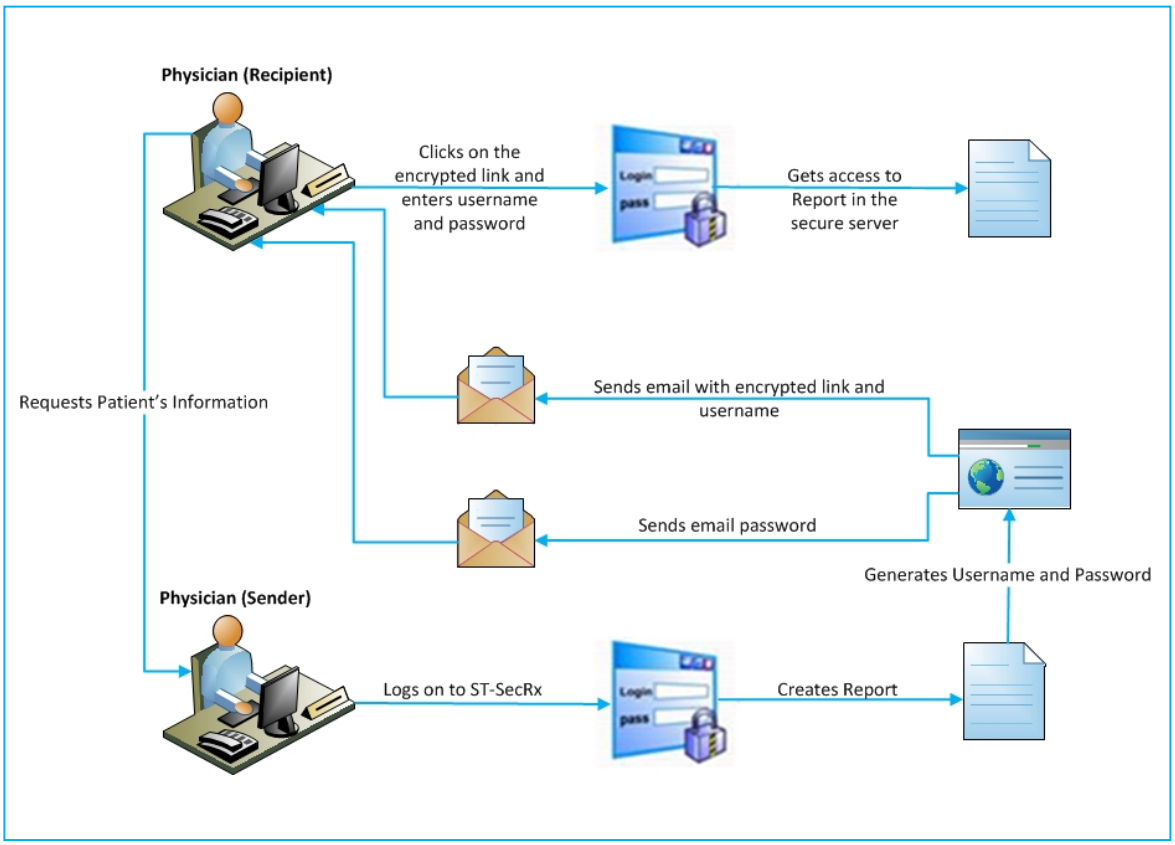


Figure 3: System Architecture of ST-SecRx

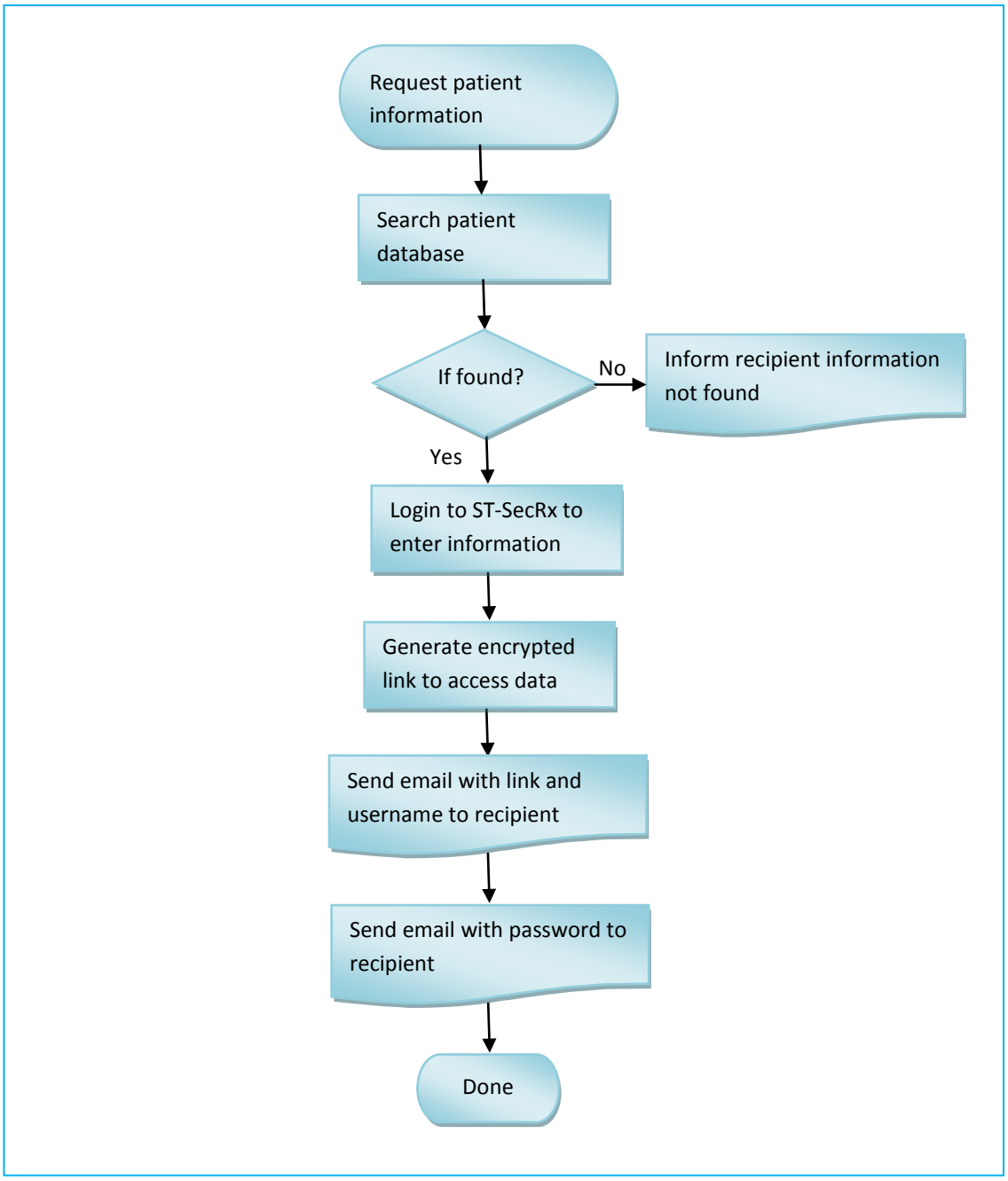


Figure 4: Workflow Diagram of ST-SecRx for Sending Information

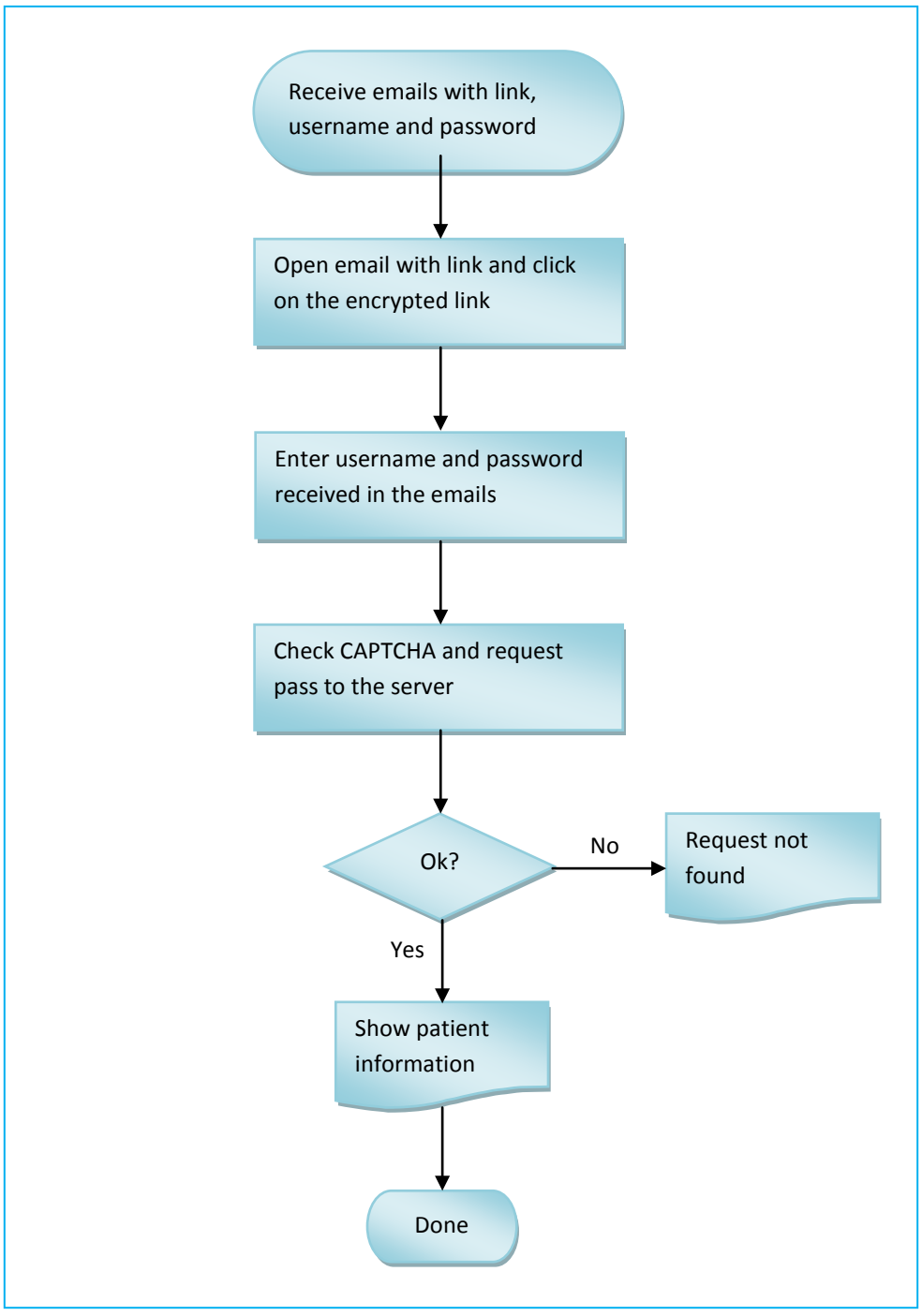


Figure 5: Workflow Diagram of ST-SecRx for Viewing Information by Recipient

It is important to note that while Transport Layer Security (TLS) or its predecessors Secure Socket Layer (SSL) and a PKI provide a high level of security for the data exchanges, all these technologies were not implemented in ST-SecRx since it was designed as a proof of concept. ST-SecRx was designed only for demonstration and testing purpose to simulate secure communication between physicians while exchanging sensitive patient data through email. The simulation achieved through the system was meant to determine and measure response of physicians to the use of secure email or similar communication tools for exchanging patient data. The encryption software would be installed if a real similar system were to be installed for use in a clinic or hospital setting.

TLS and SSL are cryptographic protocols to provide secure communication over the Internet. SSL or the more recent version TLS, is based on public key technique that provides data security for client-server communication over the Internet to prevent tampering or hacking (Yaping & Weiqi, 2001). The TLS or SSL protocol is widely used on the World Wide Web, in a variety of applications including web browsing, emails, voice over Internet protocol (VOIP), web servers etc.(Rescorla, 2001)(Lanjuan, 2006). SSL was designed by the Netscape Communication Company for encrypting TCP/IP (Transmission Control Protocol/Internet Protocol) data flow (Yaping & Weiqi, 2001)(Lanjuan, 2006). SSL is not limited to only encrypting TCP/IP data flow but also includes an identity authentication mechanism (Lanjuan, 2006).

TLS or SSL technology ensures secrecy by encrypting the data transferred by the application protocol layer so it cannot be intercepted by a third party. By using encryption

algorithms and hash functions, TLS or SSL ensures integrity of information so that data can be transferred to its destination and without losing any valuable information. The client and the server are able to identify one another by certificate technology and TLS or SSL allow certificates to exchange between certificate owners to determine if the owner is a valid user (Lanjuan, 2006). TLS or SSL is extensively used in the banking, financing and telecommunication industry since large international business network servers and general Internet explorers support for SSL security architecture. SSL however affects the speed of a system and therefore before its implementation it is necessary to properly configure the machines to ensure the system is not slowed down (Lanjuan, 2006). PKI is a commonly used technique for secured communication over the Internet (Adams & Lloyd, 2002). PKI authenticates the identity of communicators by using digital signatures. PKI works around Certification Authority and a Registration Authority. While Registration Authority authenticates the users of the infrastructure, Certification Authority issues and validates digital certificates to facilitate secure communication between the sender and receiver (Adams & Lloyd, 2002). The data transmitted over the Internet is encrypted using a randomly generated symmetric key, which in turn is encrypted using the public key of the recipient of the message (Adams & Lloyd, 2002). The recipient on receiving the message over the Internet decrypts the symmetric key using his/her public key. Then the symmetric key is used to decrypt the actual data that was sent over the Internet (Adams & Lloyd, 2002).

The basic premise of PKI is that the authentication takes place from both the server end as well as the client end. In PKI, as much as the client wants to know that the

server is authenticated, the server also must know that the client has the pre-determined credentials to access the server. In such a scenario, the public client certificates are authenticated by a trust authority that the server has validated in advance. The server also has a signed public key along with a published signature authority that the client trusts (Adams & Lloyd, 2002).

The prototype was developed as a proof of concept and no actual patient data interchange took place. The purpose of using dummy data insures that such a mode of communication was acceptable for the users before commercially available encryption technology is installed in the server for enhanced data security. This is a laboratory based study to simulate user experience rather than a study using real patient data.

However, encryption of the data transfer in and out of the ST-SecRx server is important to achieve higher degrees of data security. At present, most standard email systems do not use secure authentication methods for data transfer (Mandl & Kohane, 1999). Since clinicians would be exchanging clinical patient data using this system with all the necessary data encryption and security technologies such as PKI, SSL or TLS in the server where patient data will be encrypted and stored, however briefly, will be necessary to defend against any breach during a real installation of ST-SecRx with full security capabilities.

2.1.1. Description of ST-SecRx

ST-SecRx is a prototype of a web-based system to simulate secured communication between healthcare providers while exchanging sensitive patient data

through email. It is a simple tool with a text editor to allow physicians to enter and save clinical notes in a secure database.

Physicians outside a particular physician's clinic or hospital request patient data including history and other relevant facts. The physician to whom the request has been made searches the patient history in the existing database of the clinic or hospital IT system. The physician then identifies a patient whose information along with clinical notes needs to be sent to the physician (recipient) who requested for the information. If the data are found the physician enters it into the web-based ST-SecRx system. A browser opens up with a login screen for the physician to enter his or her existing username along with password since ST-SecRx resides within their existing server.

Figure 6: Screenshot of Login Screen of ST-SecRx

Once logged in, a text editor opens up in the Admin Control Panel allows the physician to enter information about the patient in the "Report Detail" text box. The physician can both enter information by typing in the required information or copy and paste this information to the text editor of the prototype ST-SecRx.

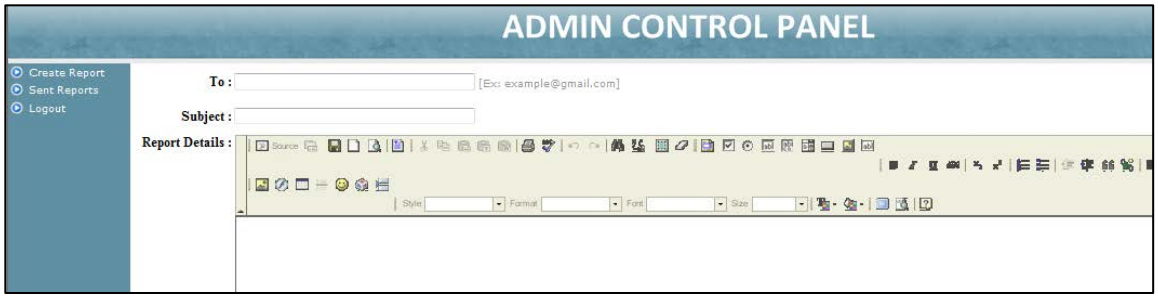


Figure 7: Screenshot of Text Editor of ST-SecRx

Once the information is entered the physician then enters the subject in the subject field. The physician has to be careful about the subject of the email. It should not contain any identifier for patient information. For example a possible subject could be: "From Dr. Smith: Information Requested by Dr. Jane Doe" implying Dr. Smith is sending the information requested by Dr. Jane Doe. To avoid entering any patient identifier inadvertently, during implementation of such a system the subject line will likely be automated without giving the physician the option of editing.

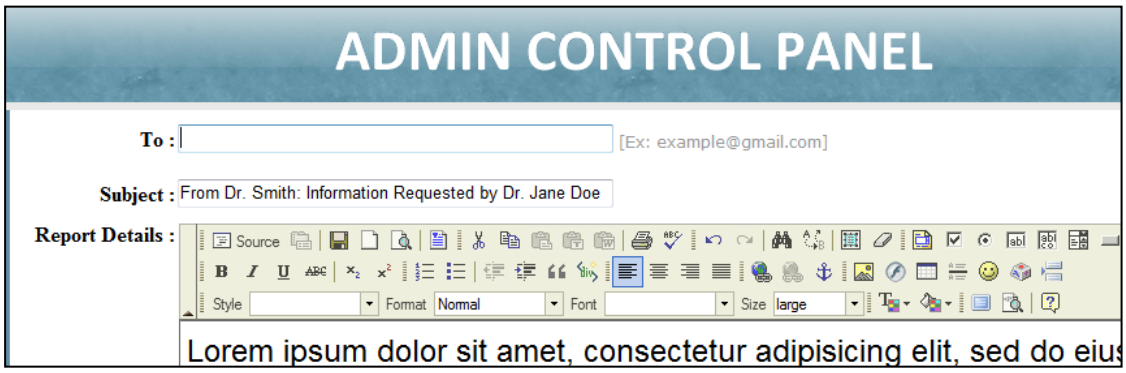


Figure 8: Screenshot of Text Editor of ST-SecRx (Adding the Subject Line)

Once the physician has entered the subject line, the next step is to enter the recipient physician's email address in the "To" field.

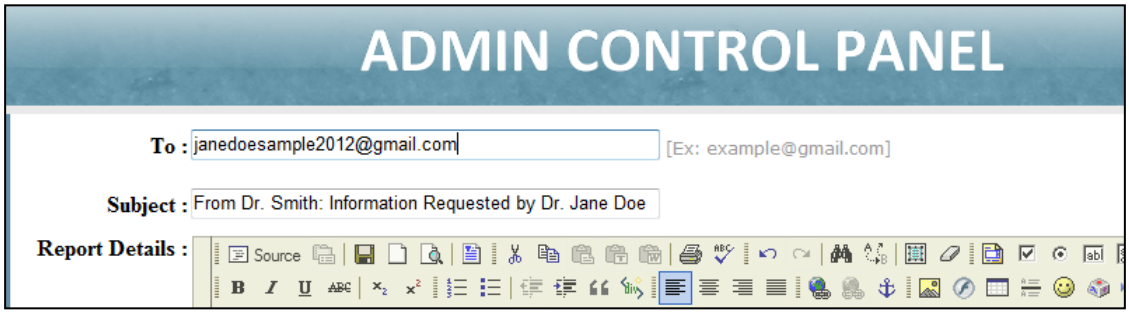


Figure 9: Screenshot of Text Editor of ST-SecRx (Adding Email Address of Recipient Physician)

The next step is to click on the "Generate Password" button to generate the username and password for the recipient physician.

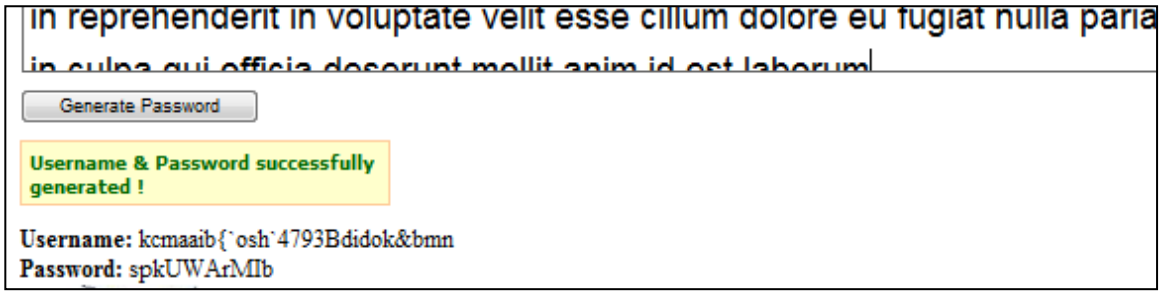


Figure 10: Screenshot of Text Editor of ST-SecRx (Generating Username and Password)

The physician then enters CAPTCHA code in the "Enter the code above here" box. CAPTCHA performs a simple math test to prevent automated software from performing actions that might mimic those of a human user. Passing through CAPTCHA improves site security and protects users. Finally, the physician clicks the send button.

Figure 11: Screenshot of Text Editor of ST-SecRx (Entering CAPTCHA Code)

Once sent, the ST-SecRx generates a hyperlink. This URL link is sent to the recipient. It should be noted that during an actual deployment this hyperlink will be generated with an encrypted parameter value that does not link itself to any patient data. This URL link will be secured by the SSL certificate if a similar software is deployed in production.

After sending information to the recipient physician the sending physician can send more reports. The physician then has to click on the "Create Report" on the left menu bar in the Admin Control Panel to open the editor to create a new report. Otherwise, the physician logs out from the ST-SecRx system.

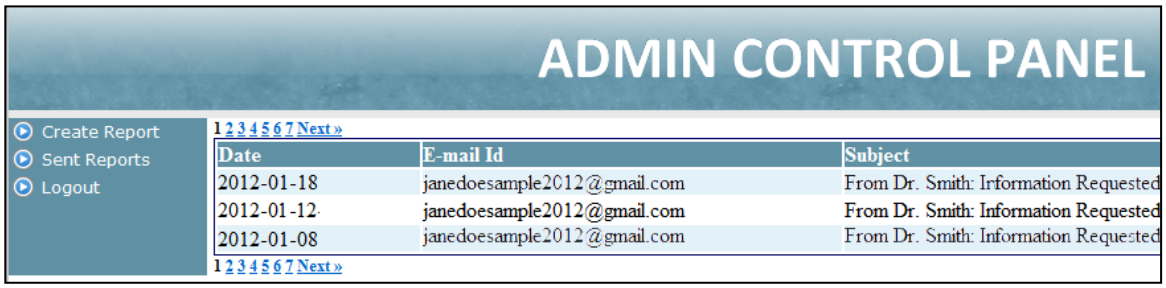


Figure 12: Screenshot of Admin Control Panel of ST-SecRx (Sent Email Box)

The recipient physician who requested the information receives two emails: one with the URL and username and a second one with the matching password. It may be noted that at the time of a real deployment, the password will be encrypted to comply with privacy and security regulations.

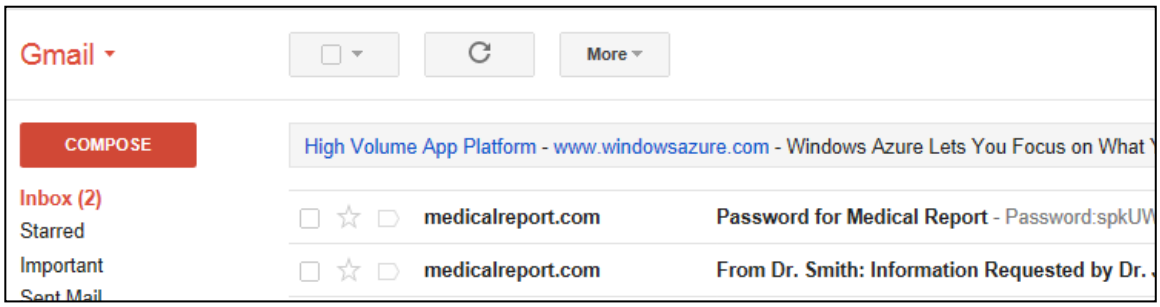


Figure 13: Screenshot of Emails Received by the Recipient Physician

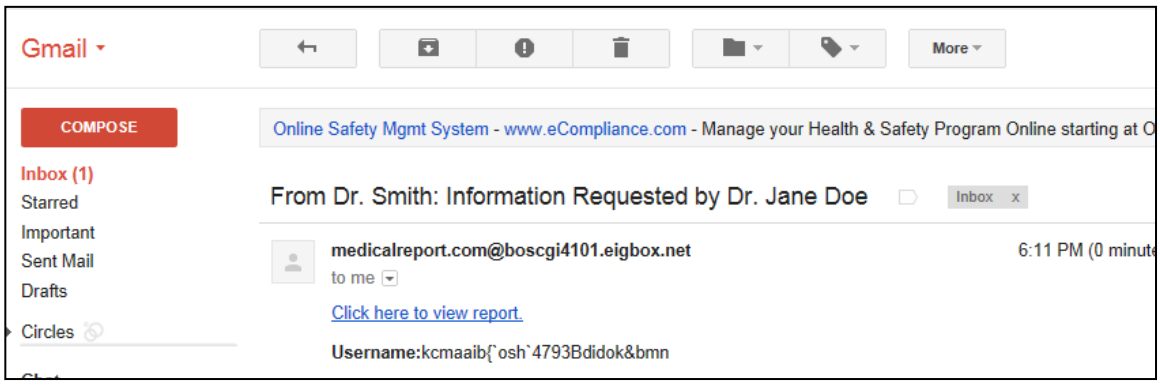


Figure 14: Screenshot of Email with Link & Username Received by the Recipient Physician

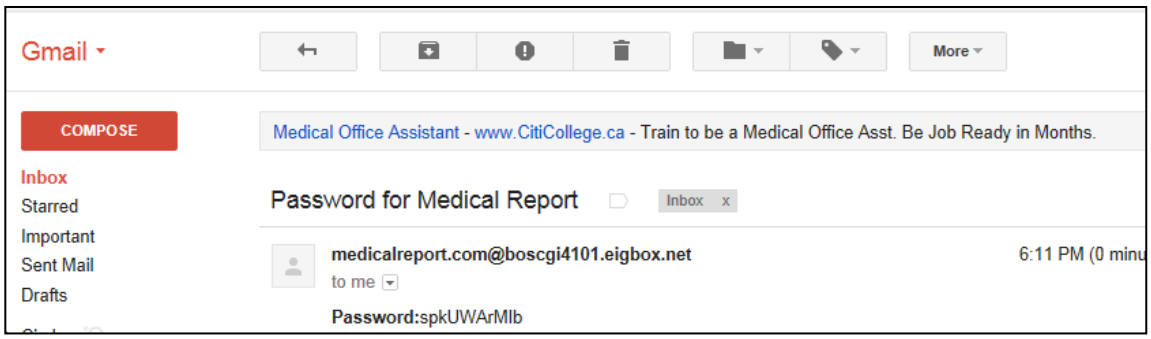


Figure 15: Screenshot of Email with Password Received by the Recipient Physician

The recipient physician clicks on the URL to view patient data. To display the information, at the prompt, a login screen opens for the recipient to enter username and password that were sent in the two separate emails.

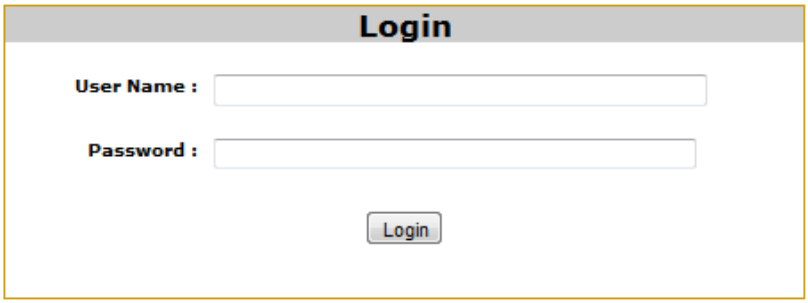


Figure 16: Screenshot of the Login Screen for Recipient Physician

As soon as the recipient enters the username and password received in the two emails the data are downloaded into his or her computer. A window opens with the patient report displaying the patient information.

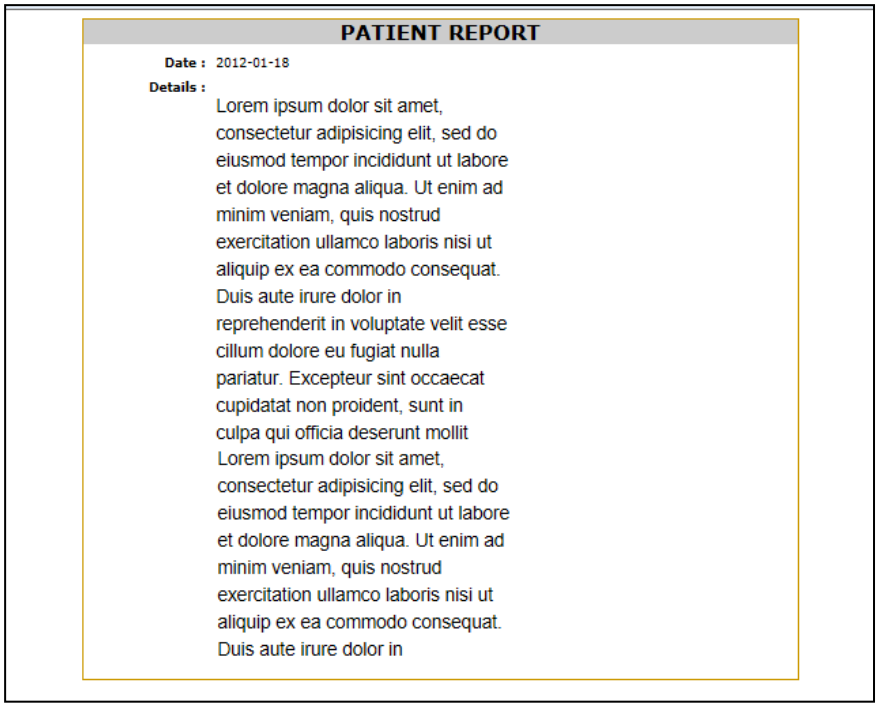


Figure 17: Screenshot of the Patient Report for Recipient Physician

2.1.2. Development and Installation of ST-SecRx

The prototype of the web-based solution, ST-SecRx was developed using PHP, a server-side, open source scripting language that is widely used for developing web-based applications. The scripts written in PHP are embedded in HTML code and executed at the server side.

The database used for all information storage is MySQL. This is a free, open source, full-featured relational database management system (RDBMS) of Oracle Corporation (MySQL, 2012). It is multi user database that can be queried using Structured Query Language (SQL). MySQL is a popular database platform, particularly for open source projects (MySQL, 2012). It supports encrypted data storage and hence was used in developing the prototype. However, for commercial projects, additional features are also available for purchase. The database software was originally developed and sponsored by a Swedish company, MySQL AB (MySQL, 2012). However, it is currently owned by Oracle Corporation, a leading US-based provider of enterprise database products (MySQL, 2012).

ST-SecRx application is currently hosted in a commercially available solution provider, Go Daddy. Go Daddy is an Internet domain registrar and hosting solution company that provide website hosting services along with enterprise level server, data and application hosting services (Go Daddy, 2012). It currently manages more than 45 million Internet domain names. Go Daddy was launched in 1997 as Jomax Technologies by entrepreneur Bob Parsons (Go Daddy, 2012). The company was later named Go Daddy and is still a privately held company (Go Daddy, 2012).

2.1 Ethics Considerations

A detailed Student Research Ethics application along with supporting documents was submitted to Hamilton Health Sciences/Faculty of Health Sciences Student Research Committee of the Research Ethics Board (REB) of McMaster University for ethics review and approval. After reviewing the application the REB informed us that the current research falls under TCPS2 (2nd edition of Tri-Council Policy Statement: Ethical Conduct for Research Involving Humans) guidelines for Program Evaluation (TCPS2 Article 2.5, p.20) and does not require REB review or approval (CIHR and NSERC and SSHRC, 2010). A copy of the letter from the REB is available in Appendix A of this document.

2.2 Inviting Physicians To Use ST-SecRx and Participate in a Survey

Physicians from hospitals, clinics and other healthcare facilities in the province of Ontario, Canada were invited to use the prototype ST-SecRx and participate in a study to examine the acceptability of the prototype. While some physicians were contacted from publicly available lists, others were known to the investigators or were referred by other physicians who agreed to participate in the study. The study period was from January, 2012 to August, 2012.

Physicians were contacted by email, a telephone call, or both and were requested to use the prototype ST-SecRx. They were given the option of either receiving an email with two URLs (hyperlink) and to review the online software or a face-to-face interview

to demonstrate ST-SecRx and collect their feedback for the survey. A detailed step-by-step user instruction guide was emailed to physicians or a printed copy was hand delivered to help walk them through the software. Additionally, some physicians received an email with the survey questionnaire and a consent form to ask them to participate in the study. Face-to-face interviews and demonstrations were conducted with the physicians in their offices. A copy of the user guideline, the survey and the consent form are in Appendix B, C and D respectively. Sample emails that were sent to physicians to request them to participate in the study appear in Appendix E of this document.

The survey was conducted from January 2012 to August 2012 and was made available both in printed format as well as online. The online survey was administered using LimeSurvey, hosted at McMaster University. The majority of the physicians received an email with two URLs. The first URL was to access and use ST-SecRx. The second URL was to complete the online survey after having used ST-SecRx. Physicians who were given a demonstration of the software in their offices responded to the survey questions after they had used ST-SecRx.

2.3 Survey

A survey was designed to assess the acceptability of ST-SecRx among physicians and their perceptions of the usefulness of the software. (see Appendix C) Questions were designed from previous research studies on healthcare and information technology (Archer & Cocosila, 2011)(Venkatesh, Morris, Gordon B. Davis, & Davis, 2003)(Featherman & Pavlou, 2003). The survey questions were first reviewed by

Samprasad Majumdar, a retired statistician who recommended changes. The changes were incorporated and subsequently the survey was reviewed by Dr. Ann McKibbon, Associate Professor, Department of Clinical Epidemiology and Biostatistics, McMaster University. Under her guidance the survey questions were further modified. It was then sent to Dr. Tapas Mondal, a pediatrician as well as Associate Professor, Department of Pediatrics, McMaster University for review. He did not recommend any changes and thought the survey questions were adequate and relevant for the proposed study.

The survey was categorized into 5 sections involving 12 questions, with some questions having sub sections. The first section involved 3 demographic questions: age range, gender, and occupation. The second section included 2 questions on the current form of communication used by the survey participants for exchanging patient information. The third section concerned factors that would facilitate the use of the prototype ST-SecRx. The fourth section was on perceived usefulness of the prototype. The fifth section was on behavioral intention to use ST-SecRx. Finally, the participants were asked about the features they liked the most, and the least, and their willingness to pay for such service.

The majority of the questions were statements with sub-questions that required participants to respond using a 5-point Likert scale where the values ranged from strongly agree (5), moderately agree (4), neither agree nor disagree (3), moderately disagree (2), strongly disagree (1). Some of the questions were multiple choice questions and some had comments provision. s. While some questions were polar questions that required a response of Yes/No, several others were open ended and allowed short, free-text

responses. For some questions depending on the response, physicians were led to additional questions. Table 1 showcases the survey questions.

Table 1: Survey Question Types

Category	Number of Questions	Number of Sub Questions	Type of Response
General Demographic Questions	3	-	Multiple Choice Multiple Choice with comments
Current Form of Email Used For Exchanging Patient Information	2	-	Yes/No
Dependent Question on Current Form of Email Used For Patient Data Exchange	1		Short free text
Factors That Would Facilitate Use of ST-SecRx	1	4	5 Point Likert Scale: Strongly Agree (5) Moderately Agree (4) Neither Agree Nor Disagree (3) Moderately Disagree (2) Strongly Disagree (1)
Perceived Usefulness of ST-SecRx	1	2	5 Point Likert Scale: Strongly Agree (5) Moderately Agree (4) Neither Agree Nor Disagree (3) Moderately Disagree (2) Strongly Disagree (1)
Behavioral Intention To Use ST-SecRx	1	6	5 Point Likert Scale: Strongly Agree (5) Moderately Agree (4) Neither Agree Nor Disagree (3) Moderately Disagree (2) Strongly Disagree (1)
Feature Liked The Most	1	-	Short free text
Feature Like The Least	1	-	Short free text
Willingness To Pay	1	-	Yes/No
Dependent Question on Willingness to Pay	1	-	Short free text

Questions were not mandatory and the participant had the option of leaving the survey unanswered at any point in time if he or she so desired. Written consent was obtained from those who responded on the paper copy of the survey. For those who participated in the online survey, participants read through a statement and confirmed their consent through their participation in the survey.

3. RESULTS AND DATA ANALYSIS

Data were collected from 22 physicians from various hospitals, clinics and other healthcare facilities across the province of Ontario, Canada. Eliminating questionnaires with no response resulted in 19 valid responses for data analysis. While some physicians were contacted from publicly available lists, others were known to the investigators or were referred by physicians who agreed to participate in the study. As a result, the exact number of physicians who were invited to participate in the study is not available.

3.1. Survey Results

Demographic Characteristic of Respondents: Of the 19 physicians who completed the survey, 79% were men, 15.8% were women and 5.3% chose not to disclose their sex. From Table 2 it is evident that 15.8% were in the age group of less than 30 years old 21.1% were in the age group of 30-39 years, 42.1% of the participants were in the age bracket of 40-49 years 15.8% were in the age group of 50-60 years, and 5.3% were 60 plus years old. Of the 19 participants, seven each were primary care physicians,

and specialists, three were residents, one was a hospitalist, and one did not answer. Demographics of the participants are presented in Table 2.

Table 2: Demographics of Respondents

Sample Size	n=19
Sex	
Men	15 (79%)
Women	3 (15.8%)
Sex Not Disclosed	1 (5.3%)
Age Group	
<30 Years	3 (15.8%)
30-39 Years	4 (21.1%)
40-49 Years	8 (42.1%)
50-59 Years	3 (15.8%)
>60 Years	1 (5.3%)
Occupation	
Primary Care Physicians	7 (36.8%)
Specialists	7 (36.8%)
Other Physicians	4 (21.1%)
Occupation Not Disclosed	1 (5.3%)

Table 3 shows the breakdown of respondents by age and sex. Of the 15 male respondents, 13.3% were in the group less than 30 years, 26.7% were in the age group 30-39 years, 40% were in the age bracket 40-49 years,, 13.3% e in the group 50-60 years, and only 6.7% were in the 60 plus group. The three female respondents were from less than 30 years, (40-49) years and (50-59) years age brackets respectively.

Table 3: Breakdown of Demographics of Respondents Based on Age Group and Sex

Age Group	Men n=15	Women n=3	Sex Not Disclosed n=1
<30 Years	2 (13.3%)	1 (33.3%)	-
30-39 Years	4 (26.7%)	-	-
40-49 Years	6 (40.0%)	1 (33.3%)	1 (100%)
50-60 Years	2 (13.3%)	1 (33.3%)	-
>60 Years	1 (6.7%)	-	-

From Table 4, out of the 15 male respondents, 46.7% were primary care physicians, 33.3% were specialists, and two were residents and one was a hospitalist. Among the three female respondents two were specialists and one was a resident.

Table 4: Breakdown of Demographics of Respondents Based on Occupation and Sex

Occupation	Men n=15	Women n=3	Sex Not Disclosed n=1
Primary Care Physicians	7 (46.7%)	-	-
Specialists	5 (33.3%)	2 (66.7%)	-
Other Physicians	3 (20.0%)	1 (33.3%)	-
Occupation Not Disclosed	-	-	1 (100%)

Current Form of Email Used for Exchanging Patient Information: Table 5 represents two questions related to the current form of email used by physicians for exchanging patient information. Of the 19 respondents, 57.9% acknowledged that they use email system provided by their organization for exchanging sensitive patient data, while 36.8% said they did not use such methods. While the majority (84.2%) of the respondents did not use an email service or a web messaging service that let them send sensitive patient data securely amongst registered users, 10.5% did use such service. One of the respondents mentioned having used a system called Medportal.

Table 5: Current Form of Email Used For Exchanging Patient Information

Current Form of Email Used For Exchanging Patient Information	Sample Size (n=19)		
	Yes	No	Did Not Answer
Using Email Provided by Organization or Exchanging Sensitive Patient Data	11 (57.9%)	7 (36.8%)	1 (5.3%)
Using Email or Web Messaging Service To Send Sensitive Patient Data Securely Between Registered Users	2 (10.5%)	16 (84.2%)	1 (5.3%)

Further analysis of Table 5 by age, sex and discipline showed some interesting results. Among those who used email systems provided by their organizations, 71%

were specialists and 50% or more were less than 60 years old. (Table 14 and 15 in Appendix F)

Once physicians had used the prototype ST-SecRx, they were asked which factors would facilitate their use of the prototype, perceived usefulness of the prototype and behavioral intention to use ST-SecRx. Finally, the participants were asked about the features they liked the most and the least and their willingness to pay such tool. For the purpose of analyzing the data, for some tables we combined the results of "strongly agree" and "moderately agree" and used the term "Agree". For "strongly disagree" and "moderately disagree" the corresponding term used for analysis was "Disagree".

Factors That Would Facilitate the Use of ST-SecRx: Table 6 lists the 4 factors that would potentially facilitate the use of the prototype ST-SecRx.

Table 6: Factors That Would Facilitate Physicians Use of ST-SecRx

Factors That Would Facilitate The Use of ST-SecRx	Sample Size (n=19)			
	Agree*	Neither Agree Nor Disagree	Disagree**	No Answer
Ease of Use	15 (79%)	1 (5.3%)	1 (5.3%)	2 (10.5%)
Not having to use an email different from the email provided by your employer for exchanging sensitive patient data	14 (73.7%)	2 (10.5%)	1 (5.3%)	2 (10.5%)
Not having to create / reset and remember a New Password Every 3/6 months for using an email different from the email provided by your organization	15 (79%)	1 (5.3%)	1 (5.3%)	2 (10.5%)
My confidence/ sense of security that my data transfer complies with regulations related to privacy and security of patient information	14 (73.7%)	3 (15.8%)	1 (5.3%)	1 (5.3%)

Agree = Strongly Agree or Moderately Agree
** Disagree = Strongly Disagree or Moderately Disagree

It is evident from Table 6 that most of the physicians (from 73.7 to 79%) agreed that these four factors would facilitate their use of ST-SecRx. A small percentage disagreed, some (from 5.3% to 15.8%) remained neutral, and a few were reluctant to answer the question. Additional analysis of Table 6 by age, sex and discipline did not show any differences in their enthusiasm for using the system. (Table 16, 17, 18 and 19 in Appendix F)

Perceived Usefulness of ST-SecRx: Physicians who used ST-SecRx were asked two questions about their perceived usefulness of the prototype. Results are presented in Table 7. More than half of the of the physicians agreed that ST-SecRx was more secure and easier to use when compared to previously used methods of patient data exchange through email. A very small percentage disagreed, some were impartial, and neither agreed nor disagreed, and a few did not answer. Further analysis by age, sex and profession showed while most men agreed with the usefulness of the prototype, a little more than 20% of the men had neutral responses for these two perceived usefulness question (Table 20 and 21 in Appendix F)

Table 7: Perceived Usefulness of ST-SecRx

Perceived Usefulness of ST-SecRx	Sample Size (n=19)			
	Agree*	Neither Agree Nor Disagree	Disagree**	No Answer
ST-SecRx is more secure compared to previously used methods of patient data exchange through email	12 (68.4%)	3 (15.9%)	1 (5.3%)	2 (10.5%)
ST-SecRx is easy to use compared to previously used methods of patient data exchange through email	10 (52.6%)	5 (26.3%)	1 (5.3%)	3 (15.8%)

* Agree = Strongly Agree or Moderately Agree
** Disagree = Strongly Disagree or Moderately Disagree

Behavioral Intention to Use ST-SecRx: Table 8 lists the six questions related to the intention of the physicians if they were able to use ST-SecRx. For each of the six questions most of the physicians (from 57.9% to 73.7%) agreed with the statement. A smaller percentage was neutral and few disagree or did not answer. Additional analyses by sex, age, and their disciplines (Tables 22, 23, 24, 25, 26, and 27 in Appendix F) did not show any substantial change in this pattern for any of the 6 questions.

Table 8: Behavioral Intention to Use ST-SecRx

Behavioral Intention to Use ST-SecRx	Sample Size (n=19)			
	Agree*	Neither Agree Nor Disagree	Disagree**	No Answer
If ST-SecRx is available to me, I intend to take advantage of it when exchanging patient data	14 (73.7%)	3 (15.8%)	1 (5.3%)	1 (5.26%)
If ST-SecRx is available to me, I am likely to use it more often than other means of patient data exchange through email	13 (68.4%)	2 (10.5%)	2 (10.5%)	2 (10.5%)
If ST-SecRx is available to me, I intend to use this as the ONLY means of exchanging patient data through email	12 (63.2%)	4 (21.1%)	2 (10.5%)	1 (5.36%)
If ST-SecRx is available to me, I am likely to use ONLY this as means of patient data exchange through email	14 (73.7%)	2 (10.5%)	2 (10.5%)	1 (5.3%)
Use of ST-SecRx would enhance my effectiveness in managing my patients' health care	12 (63.2%)	5 (26.3%)	1 (5.3%)	1 (5.3%)
Use of ST-SecRx would reduce duplication of requests for diagnostic tests between different healthcare providers	11 (57.9%)	4 (21.1%)	3 (15.8%)	1 (5.3%)

* Agree = Strongly Agree or Moderately Agree
** Disagree = Strongly Disagree or Moderately Disagree

Features Liked the Most: Eighty four percent of the physicians responded when asked about the features they liked the most and liked the least. From their responses it is

evident that the simplistic nature of the software was liked by more than half of the respondents who found it easy to use. Data encryption and security were also some of the features liked by approximately 25% of the physicians. One of the physicians also appreciated the fact that it was fast and easy to set up. The ability of the software to integrate with the emails the physicians use was a feature liked by a physician. Another physician thought the layout and the style were similar to Gmail and Microsoft Word. Using their existing user ids and passwords was also appreciated by a physician.

Features Liked the Least: About 63% responded to the question on the features they like the least. Among the many features disliked by the physicians, one was the long user name and password that the system generated for the target physician. Another feature disliked by a physician was that the system allowed the physicians only to send data to target physicians but did not allow them to both send and receive. Sending two separate emails to the recipient for username and password was also disliked by a physician. Multiple email links feature was also not liked by a physician. Two physicians thought too many steps were involved in using ST-SecRx. Three physicians did not like ST-SecRX because it was yet another online website involving email programs. Safety was another concern for one physician.

Willingness to Pay: Table 9 reflects the willingness of the physicians to pay for ST-SecRx based on age, sex and occupation. Overall about 42% were willing to pay while 36.8% were reluctant to pay. About 47% of the men were willing to pay for ST-SecRx while 33.3% were reluctant to pay. Out of the three women physicians, only one was willing to pay. As far as age groups are concerned, those in the age bracket 40-49

appeared to be quite (62.5%) willing to pay for ST-SecRx. More than 50% of both the primary care physicians and specialists were willing to pay for the system. Only five of those who were willing to pay said they would pay between $5 and $20 per month for such service.

Table 9: Willingness to Pay Based on Sex, Age Group and Occupation

Willingness to Pay	Sample Size	Yes	No	Did Not Answer
All Respondents	n=19	8 (42.1%)	7 (36.8%)	4 (21.1%)
Sex				
Men	n=15	7 (46.7%)	5 (33.3%)	3 (20%)
Women	n= 3	1 (33.3%)	2 (66.7%)	-
Sex Not Disclosed	n= 1	-	-	1 (100%)
Age Group				
<30 Years	n=3	-	2 (66.7%)	1 (33.3%)
30-39 Years	n=4	1 (25%)	3 (75%)	-
40-49 Years	n=8	5 (62.5%)	1 (12.5%)	2 (25%)
50-59 Years	n=3	1 (33.3%)	1 (33.3%)	1 (33.33%)
>60 Years	n=1	1 (100%)	-	-
Occupation				
Primary Care Physicians	n=7	4 (57.1%)	2 (28.6%)	1 (14.3%)
Specialists	n=7	4 (57.1%)	2 (28.6%)	1 (14.3%)
Other Physicians	n=4	-	3 (75%)	1 (25%)
Occupation Not Disclosed	n=1	-	-	1 (100%)

3.2.Data Analysis Using Descriptive And Inferential Statistics

The data collected from the survey were further analyzed using descriptive and inferential statistics. Based on the survey question types as described in Table 1, and the responses received from the physicians, 11 variables were identified from a pool of variables which were expected to have significant results when analyzed.

Table 10: Variables Used for Data Analysis

Variable	Variable Definition
#9	Use email provided by your organization for exchanging sensitive patient data.
#10	Use an email service or a web messaging service that lets you send sensitive patient data securely between registered users
#12	Ease of Use
#13	Not having to use an email different from the email provided by your employer for exchanging sensitive patient data.
#14	Not having to create / reset and remember a New Password Every 3/6 months for using an email different from the email provided by your organization.
#15	My confidence/ sense of security that my data transfer complies with regulations related to privacy and security of patient information.
#16	St-SecRx is more secure compared to previously used methods of patient data exchange through email
#17	ST-SecRx is easy to use compared to previously used methods of patient data exchange
#18	If ST-SecRx is available to me, I intend to take advantage of it when exchanging patient data
#22	Use of ST-SecRx would enhance my effectiveness in managing my patients' health care
#23	Use of ST-SecRx would reduce duplication of requests for diagnostic tests between different healthcare providers

From the analysis in the previous section it is evident that demographics (age, sex and occupation) did not play a major role on the outcome of the responses for survey questions, hence we excluded the demographic variables. Also from Table 8 it was apparent that the responses for all the 6 questions on behavioral intention to use ST-SecRx were somewhat similar. So we included only 3 questions from this table. The remaining variables are listed in Table 10.

Statements required participants to respond using a 5-point Likert scale where the values ranged from strongly agree (5), moderately agree (4), neither agree nor disagree (3), moderately disagree (2), strongly disagree (1). Table 11 shows descriptive statistics for the 11 variables defined in Table 10.

Given the small data size, we used Spearman's rank correlation coefficient to determine the relationship among the 11 variables and to test if there is any significant relationship among them. Computing Spearman's rank correlation coefficient for significance for two tailed test at level of significance $\alpha = 0.01$ we obtained Table 12.

Table 11: Descriptive Statistics on the 11 Variables Defined in Table 10

Descriptive Statistics					
Variables	**N**	**Minimum**	**Maximum**	**Mean**	**Std. Deviation**
# 9	18	1	2	1.39	.502
#10	18	1	2	1.89	.323
#12	17	2	5	4.35	.862
#13	17	2	5	4.35	.931
#14	17	2	5	4.47	.874
#15	18	2	5	4.22	.943
#16	17	1	5	4.29	1.160
#17	16	2	5	3.81	.911
#18	18	1	5	4.11	1.079
#22	18	2	5	4.06	.998
#23	18	2	5	3.78	1.114

Following Bell *et al*, the critical value($r_{s(CRIT)}$) for Spearman's Rank Correlation coefficient for significance for two-tailed probabilities was set at $r_{s(CRIT)} = 0.625$ when the level of significance $\alpha = 0.01$ (Belle, Fisher, Heagerty, & Lumle, 2004). If for any two variables, $r_s \geq r_{s(CRIT)}$ it can be ascertained that a significant correlation exists between the variables (Currell & Dowman, 2009).

Table 12: Spearman's Rank Correlation Coefficient (rs) For Two-Tailed Test

Spearman's Rank Correlation Coefficient(r_s)												
Variables		**# 9**	**#10**	**#12**	**#13**	**#14**	**#15**	**#16**	**#17**	**#18**	**#22**	**#23**
# 9	Correlation Coefficient	1.000	.282	.042	.113	.015	.321	.266	.292	.329	.187	.353
	Sig. (2-tailed)		.257	.873	.665	.955	.193	.303	.272	.182	.457	.150
	N	18	18	17	17	17	18	17	16	18	18	18
#10	Correlation Coefficient	.282	1.000	.290	.295	.396	.185	.022	-.302	-.365	-.363	-.230
	Sig. (2-tailed)	.257		.259	.251	.116	.463	.934	.256	.137	.139	.359
	N	18	18	17	17	17	18	17	16	18	18	18
#12	Correlation Coefficient	.042	.290	1.000	.875**	.371	.432	.142	-.021	.241	.338	.200
	Sig. (2-tailed)	.873	.259		.000	.142	.083	.588	.939	.351	.185	.441
	N	17	17	17	17	17	17	17	16	17	17	17
#13	Correlation Coefficient	.113	.295	.875**	1.000	.402	.661**	.272	-.090	.174	.225	.039
	Sig. (2-tailed)	.665	.251	.000		.110	.004	.292	.740	.505	.385	.883
	N	17	17	17	17	17	17	17	16	17	17	17
#14	Correlation Coefficient	.015	.396	.371	.402	1.000	.370	.286	-.280	-.091	-.113	-.050
	Sig. (2-tailed)	.955	.116	.142	.110		.143	.265	.293	.729	.665	.848
	N	17	17	17	17	17	17	17	16	17	17	17
#15	Correlation Coefficient	.321	.185	.432	.661**	.370	1.000	.711**	.081	.314	.436	.131
	Sig. (2-tailed)	.193	.463	.083	.004	.143		.001	.765	.205	.071	.604
	N	18	18	17	17	17	18	17	16	18	18	18
#16	Correlation Coefficient	.266	.022	.142	.272	.286	.711**	1.000	.280	.448	.556	.087
	Sig. (2-tailed)	.303	.934	.588	.292	.265	.001		.293	.071	.021	.739
	N	17	17	17	17	17	17	17	16	17	17	17
#17	Correlation Coefficient	.292	-.302	-.021	-.090	-.280	.081	.280	1.000	.544	.350	.292
	Sig. (2-tailed)	.272	.256	.939	.740	.293	.765	.293		.029	.183	.273
	N	16	16	16	16	16	16	16	16	16	16	16
#18	Correlation Coefficient	.329	-.365	.241	.174	-.091	.314	.448	.544	1.000	.817**	.813**
	Sig. (2-tailed)	.182	.137	.351	.505	.729	.205	.071	.029		.000	.000
	N	18	18	17	17	17	18	17	16	18	18	18
#22	Correlation Coefficient	.187	-.363	.338	.225	-.113	.436	.556	.350	.817**	1.000	.698**
	Sig. (2-tailed)	.457	.139	.185	.385	.665	.071	.021	.183	.000		.001
	N	18	18	17	17	17	18	17	16	18	18	18
#23	Correlation Coefficient	.353	-.230	.200	.039	-.050	.131	.087	.292	.813**	.698**	1.000
	Sig. (2-tailed)	.150	.359	.441	.883	.848	.604	.739	.273	.000	.001	
	N	18	18	17	17	17	18	17	16	18	18	18

**. Correlation is significant at the 0.01 level (2-tailed).

From Table 12, it can be observed that 6 instances had the specified threshold of $r_s \geq r_{s(CRIT)}$ at $\alpha = 0.01$ have been reached as presented in Table 13.

Table 13: rs ≥ rs(CRIT) when α = 0.01

Variables	Variable Description	Spearman's rho (r_s)	p value
#12	Ease of Use	0.875	0.000
#13	Not having to use an email different from the email provided by your employer for exchanging sensitive patient data.		
#18	If ST-SecRx is available to me, I intend to take advantage of it when exchanging patient data	0.817	0.000
#22	Use of ST-SecRx would enhance my effectiveness in managing my patients' health care		
#18	If ST-SecRx is available to me, I intend to take advantage of it when exchanging patient data	0.813	0.000
#23	Use of ST-SecRx would reduce duplication of requests for diagnostic tests between different healthcare providers		
#15	My confidence/ sense of security that my data transfer complies with regulations related to privacy and security of patient information.	0.711	0.001
#16	ST-SecRx is more secure compared to previously used methods of patient data exchange through email		
#22	Use of ST-SecRx would enhance my effectiveness in managing my patients' health care	0.698	0.001
#23	Use of ST-SecRx would reduce duplication of requests for diagnostic tests between different healthcare providers		
#13	Not having to use an email different from the email provided by your employer for exchanging sensitive patient data.	0.661	0.004
#15	My confidence/ sense of security that my data transfer complies with regulations related to privacy and security of patient information.		

From Table 13 it can be observed that r_s between variables #12 *(Variable #12 =Ease of Use)* and #13 (*Variable #13 =Not having to use an email different from the email provided by your employer for exchanging sensitive patient data*) is 0.875 (p=0.000) which is greater than $r_{s(CRIT)}$ at $\alpha = 0.01$ level of significance. Hence we can accept a significant correlation between these two variables. In essence, it implies that a linear relation exists between these two variables such that those who though that ease of use was a factor to facilitate the use of ST-SecRx also thought that not having to use and email provided by their employer was a factor that would facilitate the use of ST-SecRx.

Using the same analogy we find from Table 13 r_s between variables #18 *(Variable #18 = If ST-SecRx is available to me, I intend to take advantage of it when exchanging patient data)* and #22 *(Variable #22 = Use of ST-SecRx would enhance my effectiveness in managing my patients' health care)* is 0.817 (p=0.000) implying once again that a significant correlation exists between the two variable at $\alpha = 0.01$. Essentially, it means that those who agreed that if ST-SecRX is available to them they would take advantage of the software in exchanging patient data also agreed if they use the software it would enhance the effectiveness in managing their patients' healthcare.

It appears from the Table 13 that between variables #18 *(Variable #18 = If ST-SecRx is available to me, I intend to take advantage of it when exchanging patient data)* and #23 *(Variable #23 = Use of ST-SecRx would reduce duplication of requests for diagnostic tests between different healthcare providers)*, the r_s = 0.813, and p=0.000, indicating the existence of a significant correlation between these two variables with $r_s \geq$

$r_{s(CRIT)}$ at $\alpha = 0.01$. In effect, those who thought that they would take advantage of ST-SecRx if it were available to them also felt that use of ST-SecRx would reduce duplication of diagnostic tests implying once again a linear relationship between the two variables.

For variables #15 *(Variable #15 = My confidence/ sense of security that my data transfer complies with regulations related to privacy and security of patient information)* and #16 *(Variable #16 = ST-SecRx is more secure compared to previously used methods of patient data exchange through email)* in Table 13, $r_s = 0.711$, and p=0.001, indicating the existence of a correlation between these two variables at $\alpha = 0.01$. Those who thought that ST-SecRx was more secure compared to previously used methods of data exchange through email also felt that the patient data transfer was more secure and complies with patient privacy and security regulations.

Some degree of correlation was observed between variables #22 *(Variable# 22 = Use of ST-SecRx would enhance my effectiveness in managing my patients' health care)* and #23 *(Variable # 23 = Use of ST-SecRx would reduce duplication of requests for diagnostic tests between different healthcare providers)* in Table 13 with $r_s = .0.698$ (p=0.001) indicating $r_s \geq r_{s(CRIT)}$ at $\alpha = 0.01$. Physicians who were of the opinion that using ST-SecRx would enhance the effectiveness on managing their patients' healthcare also believed that it would reduce duplication of diagnostic tests.

Finally from Table 13 it may be observed that r_s between variables #13 (*Variable #13 =Not having to use an email different from the email provided by your employer for*

exchanging sensitive patient data) and #15 *(Variable #15 = My confidence/ sense of security that my data transfer complies with regulations related to privacy and security of patient information),* is 0.661 (p=0.004) implying once again that specified threshold for $r_s \geq r_{s(CRIT)}$ has been reached and there is some degree of correlation between these two variables at $\alpha = 0.01$. It appears that a linear relationship exists between these two variables. Physicians, who felt it would facilitate their use of ST-SecRx if they do not have to use an email different from the email provided by their employer for exchanging patient data, also seems to agree that data transfer using ST-SecRx complies with regulations related to privacy and security of patient information.

3.3. Comments of Physicians

While interviewing and demonstrating the software, six of the physicians whom I met in person and another five physicians who responded to the online survey said that they found ST-SecRx easy to use and said they would use it in their offices if it was available and proven secure. Four of the physicians whom I met in person and also those who responded to online survey thought that the software would enhance security of patient information being sent through the Internet.

Four physicians at the time of interview and two (who participated in the online survey) expressed their dissatisfaction with the one way data transfer and the long username and password which they found awkward. Two physicians were also disappointed that they had to test the software both as a sender and as recipient because of the one way communication feature of the tool.

Six physicians whom I met in person suggested that ST-SecRx should allow physicians to attach reports, diagnostic test results, digital images, prescriptions and clinical notes. Four physicians whom I met in person thought that by adding a list of approved senders/recipients, the system could prevent sending patient information to unauthorized recipients unintentionally.

While all of the six physicians met in person and five of the physicians who responded to the online survey appreciated the simplicity and ease of use of the ST-SecRx system, three physicians expressed their concern about using yet another system in their practice. They felt they were already overloaded with too many robust systems and adding another system would reduce the time they spent with their patients. Sending two separate emails to the recipient for username and password was thought to be cumbersome by one physician. The same physician thought that the instructions in the two emails were incomplete and a third email would be required to explain to the recipient physician about receiving two emails with the link, username and password. Otherwise they might delete the mails as spam mails.

One of the physicians thought that other than accepting on face value that the ST-SecRx is safe, the physician had his doubts about ST-SecRx's claim of being a safe and secure means for data transfer. The same physician also thought that it was important to know how safe the system actually was and how different it was from using hospital emails for sending patient data. Another physician said that only time would tell how good ST-SecRx was. Two physicians said that they did not use email in their practice.

All the six physicians whom I met in person and two of those who responded to the online survey expressed their concern about lack of proper instructions in the email to view the information sent to the recipient and also that the process involved too many steps. The 6 participants whom I met in person also felt that they had to spend more time than anticipated to decipher how to use the system. While testing the software, these physicians had to refer to the user manual several times rather than following the instructions on the email.

4. DISCUSSION

To explore an alternative method of secure data exchange of patient information among physicians and collecting the data on physicians' perceptions of using email to exchange confidential email, the simulated system ST-SecRx was developed as an interim solution. The prototype, ST-SecRX, was never meant to be a production system to be used with live data. Rather, it was developed as an interim solution to explore the scope of secure communication between healthcare providers while exchanging sensitive patient data through email. It has been designed to be a simple tool with a text editor to allow physicians to enter and save clinical notes in a secure database and to allow transfer of encrypted data. The prototype as it stands now does not meet existing privacy and security standards since it was developed only as a proof of concept to simulate secure communication between physicians while exchanging sensitive patient data through email. Technologies such as Transport Layer Security or its predecessors Secure Socket Layer and a Public Key Infrastructure to provide a high level of security for the data

exchanges were not implemented in the prototype. However, during an actual deployment of similar system these technologies will be implemented to comply with security and privacy regulation.

The survey showed that the simulated ST-SecRx was well received among the physicians who used it. Their high interest in the prototype ST-SecRx system and their intention to use a similar system if it were put into commercial production is evidenced from their response on the survey. ST-SecRx was successful in its mission to simulate a real-life environment for clinical data exchange and record responses from physicians on the utility of such a system. It appears that a demand exists among the physicians studied for a system such as ST-SecRx for exchanging sensitive patient data while complying with privacy regulations.

Physician satisfaction with the simulated ST-SecRx was associated with the simplicity of the software for sending patient data in a secure way. Physicians generally perceived the prototype to be useful and found it to be easy to use, easy to set up, fast and secure. The physicians found it usable and appreciated that it would substantially enhance their effectiveness in managing their patients' healthcare. Participants realized that patient data being sent in an encrypted format through email was a better way for sending patient information than sending information in the general body of an email. Physicians also acknowledged that the simulated methods of ST-SecRx was more secure compared to previously used methods of data exchange using regular email and the use of encryption technology increased confidence and a sense of security among the physicians.

The ability of the simulated environment created by ST-SecRx to integrate with common email applications that most people use was greatly appreciated and a similar method if used in conjunction with PKI, SSL and TLS technologies in production has a high possibility of adoption. One of the reasons that many physicians looked favorably on a realistic solution such as the simulated ST-SecRx was that this would integrate seamlessly with the email system provided by their employer. It would not also require using a different email system or having to periodically create or reset and remember new passwords. Using a system similar to the simulated ST-SecRx, according to the physicians, would reduce duplication of requests for diagnostic tests between different healthcare providers. One immediate positive outcome of using a similar system would be a possible reduced cost of healthcare.

The current research approach may indicate a reduction in the cost of care by making patient information available to service providers who then can make clinical decisions more quickly. The results from the study suggest that physicians believed that a system like the simulated ST-SecRx would be capable of reducing duplication of diagnostic tests. The simulated system is flexible enough and could be implemented in any hospital, clinic or other healthcare facilities that require exchanging patient information once the necessary technologies that ensure privacy and security are deployed. Transfer of patient data could be done for consultation on treatments, transfer of the patient to other facilities, requests for consultation or advice, reporting back on consultations, general communication, and other situations.

Despite the fact that most of the physicians were pleased with the features and the seemingly usefulness of the prototype, the primary source of their dissatisfaction was that the design provided one-way communication only. While the simulated ST-SecRx allowed physicians to send information to physicians who requested such information it did not allow the recipient physician to send information back to the sender physician. Physicians expressed their concern about a lack of proper instruction in the email to view the information sent to the recipient. Participants had to spend more time than anticipated to find out how to use the system. The longer username and password were also found to be awkward to use by the physicians. The physicians surveyed were also apprehensive about safety and security of the simulated system, ST-SexRx.

4.1.Recommendations

Examining the lessons learned from past successes and failures in implementing HIT systems and the responses of the participating physicians about ST-SecRx, we realized that it is important take into consideration several challenges listed below while designing and implementing ST-SecRx for actual use in hospitals, clinics or healthcare facilities.

First of all, given the necessity to implement PKI-based security which is accepted as a standard in today's realm of data security, where senders and receivers both need to conform to a standard key installation for PKI protection, vendors providing such a solution could be recruited to provide such a solution within a region or an organization, that would be uniform in its deployment and user experience. An established vendor with

credibility in the market would be able to bring a wider group of physicians under the umbrella of one uniform security platform.

Another approach could be to recruit regional health agencies such as eHealth Ontario to modify their ONE® Mail product to better fit physician needs and therefore increase its user acceptability. A list of suggested modifications can be developed using the findings of this research that could be built into a revised ONE® Mail system. Some of the important features that were derived from the analysis of the survey results are listed below. These could be incorporated into a revised ONE® Mail system.

A key role for successfully designing and implementing such a solution would be to communicate regularly with all key stakeholders, including end users, top level management, and decision makers to gather information and to document concerns and issues regarding design, use and adoption of secure email. Subsequently, developers need to identify any problems based on user feedback about the usability of the proposed secure email system, and try to address the key issues identified by developing a prioritized list of activities and relating all activities to a desired goal.

One of the recommendations for a successful deployment and adoption among the users would be taking adequate measures to prepare users to adopt and accept changes associated with the implementation of a new system for patient data exchange.

A major task would be conducting regular usability assessments among end-users (physicians) and making necessary modification in the proposed system. It would also be important to develop an effective training program to train the users for its successful

acceptance by the users such that the five components (learnability, efficiency, memorability, errors and satisfaction) of usability are satisfied (Neilson, 2012).

To avoid the all too common frustration, stress, and disruption of workflow associated with any HIT implementation, regular training of physicians would have to be conducted in the use of the proposed secure system for data exchange. Also an IT support team would have to be organized to deal with any technical issues the physicians might encounter while using the system.

An important feature that would enhance the efficiency and quality of the system would be to add a new functionality to allow physicians to attach diagnostic test results, digital images, prescriptions and clinical notes as a part of the reports they intend to send to the recipient physicians.

Another useful measure would be to limit access privileges to the system. Only these people would be able to login to the ST-SecRx system for communicating with other healthcare providers through email. Then, based on their user type and associated user-privileges, authorized users would be granted permission to enter information into the secure database.

In order to avoid unintentional exposure of patient information to unauthorized people by inadvertently sending email to wrong addresses, a user list could be added to the proposed system. This would allow physicians to add the names and emails of the physicians to whom they intend to send the information before they actually send the information. At the time of sending the information the sender could simply select the physician's email address from a list and then send the email with the patient information.

The long username and password issue has to be addressed while keeping in mind the security of the system.

To enhance the security of the system and to avoid entering any patient information in the subject line of the mail inadvertently, the subject line could be automated without giving the physician the option of editing during a real-time deployment.

However, to address the one way communication ability of ST-SecRx, it would be necessary to consider key stakeholder decisions about the level of security they would want for their organization. A drawback of allowing the recipient physician to have permanent access to the server of the clinic, hospital or other healthcare facilities would be that such access can compromise regulatory compliance regime for the clinic's computing resources that the external physician is accessing. To avoid such a situation, introduction of an enhanced security perimeter in the architecture of the system may be necessary which will require partial re-design of the system.

4.2.Limitations

The ST-SecRx system has been developed to simulate a secure email communication environment for physicians to experience and respond to. Since ST-SecRx was designed as a proof of concept to provide interim solution, the standard security frameworks such PKI was not implemented which should be deployed before such a prototype moves to an actual production.

With respect to the analysis of the responses to the survey conducted for this purpose, one of the major limitations of this research has been the small sample size. A major challenge was to get participants to review ST-SecRx and participate in the survey. Participation involved two steps: reviewing the software and responding to the survey questions. Physicians required more time than anticipated and hence this could be one of the reasons for low participation rates.

Although the software was easy to use as reported by most of the participants, the instructions sent in the email to the recipients to view the information were deficient. This could be one of the possible causes for low response rate of the survey.

The application is currently hosted in a commercially available hostage solution provider, GoDaddy.com. Since the prototype was developed as a proof of concept to provide physicians with a temporary solution to find out if a similar mode of secure email communication is acceptable for the users, all of the recommended commercially available encryption technology and data security measures were not implemented. Stronger encryption and security measures would need to be installed if any similar actual implementation occurs.

Another limitation was that the prototype was designed for one way communication only, and did not let allow users to both send and receive information. The prototype was developed for demonstration and testing purpose so two way communication between providers was not installed. Eventually, in an actual production implementation, the software will be customized for use and hosted in the server of a clinic or a hospital setting. At the time depending on the specific requirement of the clinic

or the hospital, one way or both ways communication and or any other customization that they feel is necessary could be executed. Also, as per the privacy and security policies at the location of the implementation, in compliance with all local and national relevant regulations, necessary technology will be introduced, such as, Public Key Infrastructure, SSL, TLS etc. Once the implementation is complete, the primary stake-holders at the location will be responsible for maintaining the security infrastructure and all compliance-related issues.

The study was limited to physicians only and excluded other healthcare providers. Other healthcare providers such as nurses and pharmacists also use email to exchange patient healthcare information. Including them would have given a better perspective about ST-SecRx's acceptability among healthcare providers.

Despite the limitations, the study data provided useful insight for physicians' perceptions on the use of secure communication of patient data through email. A larger sample size would have enabled a better statistical analysis of the data and determined the significance of dependence and relationship between the variables.

5. CONCLUSION

Emphasis needs to be put on privacy, security and integrity of patient data, given the portability and accessibility of data having been magnified many times with the progress in Internet technology. Some physicians use conventional email for exchanging sensitive patient information. This use breaches patient privacy and security

considerations which is considered to be major impediment towards the use of email for exchanging healthcare data. Newer and more portable devices are becoming more popular within the physician community as preferred communication devices, even though electronic exchange of data using portable devices is not yet very common in healthcare. Under these conditions, it is a challenge for healthcare providers to exchange patient information in a secured and efficient way while fully complying with relevant regulations pertinent to the privacy and security of health information in their local jurisdictions.

The objective of this study was to provide a prototype as an interim solution to simulate secure exchange of patient data using email and examine the system's acceptability among physicians. The solution was designed using emerging technologies and changing habits of physicians who are using diverse communication devices such as smart phones, laptops, netbooks and tablet personal computers. The current research was successful in providing a potential solution to the problem by developing a prototype for secure patient data communication of web based solution called ST-SecRx. The aim of the web-based prototype, ST-SecRx, was to be a simple tool that could enable secure communication among clinicians while complying with privacy regulations. The current research was also mindful of the existence of a number of platforms through which the physicians could seek to use this website. Such platforms included hardware such as personal computers, laptops, netbooks, and tablets.

My findings revealed that a solution similar to ST-SecRx with appropriate security measures such as PKI, SSL or TLS technologies implemented could be an

improvement over conventional email because it provides security using encrypted technology and access control (Appari & Johnson, 2010)(Liederman & Morefield, 2003). However, it must be kept in mind that the ST-SecRx is a simulated prototype and any production deployment would require significant improvements in terms of implementing adequate data security infrastructure. Additionally, it did not restrict the physicians to the pre-installed email clients in their desktop machines, such as Microsoft Outlook or Eudora. Instead, this new tool, with appropriate enhancements, can enable physicians to exchange patient information through most available computing platforms, software and hardware. Participants reported that such a tool had the potential to be used because of its simple, fast, and easy to use design. Participants were likely to use a similar system that could be a secure vehicle for sending healthcare information provided all the standards for privacy and security are installed in an actual deployment. As mentioned in the recommendations part of this section, such flexibility can be kept in mind while designing a more robust and secure system as and if the simulated prototype moves into an actual deployment.

Such a system may have potential to reduce the overall cost of healthcare by reducing duplication of diagnostic tests and making patient-specific information exchange faster. The current approach could be the basis for systems that make patient data available to service providers which would facilitate providers to quickly make clinical decisions. This solution, with enhancements, could be implemented in any hospital, clinic or other healthcare facilities that require exchanging patient information. The

solution can be customized to their specific requirements and the requirements of privacy and security standards.

More research needs to be conducted with a larger sample size to validate the findings of this study. In spite of the small sample size, this study could be used by future researchers for designing a tool for exchanging patient information using email as a mode of communication. The limitations, dissatisfaction and concerns expressed by the physicians who used ST-SecRx could direct future research. The study could be extended to include other healthcare professionals exchanging sensitive clinical data.

REFERENCES

Adams, C., & Lloyd, S. (2002). *Understanding PKI Concepts, Standards And Deployment Considerations* (2nd ed.). Boston, MA: Pearson Education, Inc.

Anderson, R. (1996). Clinical system security: Interim guidelines. *BMJ (Clinical Research Edition), 312*(7023), 109-111.

Appari, A., & Johnson, M. E. (2010). Information security and privacy in healthcare: Current state of research. *Internet and Enterprise Management, 6*(4), 279-314.

Archer, N., & Cocosila, M. (2011). A comparison of physician pre-adoption and adoption views on electronic health records in Canadian medical practices. *Journal of Medical Internet Research, 13*(3), e57.

Arnold, C. W., Bui, A. A., Morioka, C., El-Saden, S., & Kangarloo, H. (2007). Informatics in radiology: A prototype web-based reporting system for onsite-offsite clinician communication. *Radiographics : A Review Publication of the Radiological Society of North America, Inc, 27*(4), 1201-1211.

Baker, L., Wagner, T. H., Singer, S., & Bundorf, M. K. (2003). Use of the internet and e-mail for health care information: Results from a national survey. *JAMA, 289*(18), 2400-2406.

Belle, G. V., Fisher, L. D., Heagerty, P. J., & Lumle, T. S. (2004). *Biostatistics: A Methodology For The Health Sciences* (2nd ed.) John Wiley & Son.

Black, A. D., Car, J., Pagliari, C., Anandan, C., Cresswell, K., Bokun, T., et al. (2011). The impact of ehealth on the quality and safety of health care: A systematic overview. *PLoS Medicine, 8*(1), e1000387.

Brailer, D. J. (2005). Interoperability: The key to the future health care system. *Health Affairs (Project Hope), Suppl Web Exclusives*, W5-19-W5-21.

Branger, P., Van't Hooft, A., & Van der Wouden, H. C. (1995). Coordinating shared care using electronic data interchange. Paper presented at the *MEDINFO: World Congress on Medical and Health Informatics 1995, , 8 Pt 2* 1669.

Branger, P., Wouden, J., Schudel, B., Duisterhout, J., Lei, J., & Bemmel, J. (1992). Electronic communication between providers of primary and secondary care. *BMJ, 305*(6861), 1068-1070.

Canada Health Infoway. (2011a). *About Canada Health Infoway.* Retrieved Aug 23, 2011, from https://www.infoway-inforoute.ca/lang-en/about-infoway

Canada Health Infoway. (2011b). *Advancements in Canada's electronic health information and communications technology systems.* Retrieved Aug 23, 2011, from https://www.infoway-inforoute.ca/about-ehr/advancements

Canada Health Infoway. (2011c). *EHRs will improve, protect, and save lives.* Retrieved Aug 23, 2011, from https://www.infoway-inforoute.ca/about-ehr

Canada Health Infoway. (2011d). *Keeping Canadians informed.* Retrieved Aug 23, 2011, from https://www.infoway-inforoute.ca/lang-en/about-ehr/public-education-campaign-about-ehr

Canada Health Infoway. (2012). *EHRS blueprint.* Retrieved October 04, 2012, from https://www.infoway-inforoute.ca/index.php/resources/technical-documents/architecture?view=docman

Canadian Healthcare Technology. (2012). *Cancer agency ordered to stop sending paper records.* Retrieved July 27, 2012, from http://www.canhealth.com/News1800.html;

Car, J., & Sheikh, A. (2004a). Email consultations in health care: 1--scope and effectiveness. *BMJ (Clinical Research Ed.), 329*(7463), 435-438.

Car, J., & Sheikh, A. (2004b). Email consultations in health care: 2--acceptability and safe application. *BMJ (Clinical Research Ed.), 329*(7463), 439-442.

Carnegie Mellon CyLab Portal. (2012). *The reCAPTCHA project.* Retrieved August 23, 2012, from http://www.cylab.cmu.edu/partners/success-stories/recaptcha.html;

Chaudhry, B., Wang, J., Wu, S., Maglione, M., Mojica, W., Roth, E., . . . Shekelle, P. G. (2006). Systematic review: Impact of health information technology on quality,

efficiency, and costs of medical care. *Annals of Internal Medicine, 144*(10), 742-752.

Canadian Institute of Health Research, and Natural Sciences and Engineering Research Council of Canada, and Social Science and Human Research Council of Canada. (2010). *Tri-council policy statement: Ethical conduct for research involving humans, December 2010.* Retrieved August 16, 2012, from http://www.pre.ethics.gc.ca/pdf/eng/tcps2/TCPS_2_FINAL_Web.pdf

Currell, G., & Dowman, A. (2009). *Essential Mathematics And Statistic For Science* (2nd ed.) John Wiley & Sons.

DePhillips, H. A. (2007). Initiatives and barriers to adopting health information technology: A US Perspective . *Disease Management & Health Outcomes, 15*(1), 1-6.

eHealth Ontario. (2012). *ONE mail.* Retrieved October 01, 2012, from http://www.ehealthontario.on.ca/en/services/one-mail

Evans, L., Nicholas, P., Hughes-Webb, P., Fraser, C. L., Jamalapuram, K., & Hughes, B. (2001). The use of e-mail by doctors in the west midlands. *Journal of Telemedicine and Telecare, 7*(2), 99-102.

Featherman, M., & Pavlou, P. (2003). Predicting e-services adoption: A perceived risk facets perspective. *International Journal of Human-Computer Studies, 59*(4), 451-474.

Gerstle, R. S. (2004). E-mail communication between pedatrician and their patients. *Pediatrics, 114*(1), 317-321.

Go Daddy. (2012). *About Go Daddy.* Retrieved August 28, 2012, from http://www.godaddy.com/newscenter/about-godaddy.aspx?ci=9079

Grogan, J. (2006, May). EHRs and information availability: Are you at risk? *Health Management Technology, 27*, 16-8,20.

Hill, J. W., Langvardt, A. W., & Massey, A. P. (2007). Law, information technology, and medical errors: Toward a national healthcare information network approach to improving patient care and reducing medical malpractice costs. *JLTP: University of Illinois Journal of Law, Technology and Policy, 2*, 1-79.

Hill, J. W., & Powell, P. (2009). The national healthcare crisis: Is eHealth a key solution? *Business Horizons, 52*(3), 265-277.

Hillestad, R., Bigelow, J., Bower, A., Girosi, F., Meili, R., Scoville, R., & Taylor, R. (2005). Can electronic medical record systems transform health care? potential health benefits, savings, and costs. *Health Affairs (Project Hope), 24*(5), 1103-1117.

Hodge, J. G. (December 2003). Health information privacy and public health. *The Journal of Law, Medicine & Ethics, 31*(4), 663-671.

Hsiao, A. L., Bazzy-Asaad, A., Tolomeo, C., Edmonds, D., Belton, B., & Benin, A. L. (2011). Secure web messaging in a pediatric chronic care clinic: A slow takeoff of "kids' airmail". *Pediatrics, 127*(2), e406-13.

Kaushal, R., Blumenthal, D., Poon, E. G., Jha, A. K., Franz, C., Middleton, B., et al. (2005). The costs of a national health information network. *Annals of Internal Medicine, 143*(3), 165-173.

Keshavjee, K. (2010, April). The eHealth Ontario scandal: Why we're still not out of the woods. *Canadian Healthcare Technology,*

Keshavjee, K., Pairaudeau, N., & Bhanji, A. (2006). Physician office readiness for managing internet security threats. *Paper Presented at the AMIA (American Medical Informatics Association.) Proceedings: Annual Symposium.AMIA Symposium,* , 981.

Kittler, A. F., Carlson, G. L., Harris, C., Lippincott, M., Pizziferri, L., Volk, L. A., et al. (2004). Primary care physician attitudes towards using a secure web-based portal designed to facilitate electronic communication with patients. *Informatics in Primary Care, 12*(3), 129-138.

Lang, E., Afilalo, M., Vandal, A. C., Boivin, J. F., Xue, X., Colacone, A., et al. (2006). Impact of an electronic link between the emergency department and family physicians: A randomized controlled trial. *CMAJ, 174*(3), 313-318.

Lanjuan, L. (2006). SCM security solution based on SSL protocol. Paper presented at the *Service Operations and Logistics, and Informatics, 2006. SOLI '06. IEEE International Conference,* 814-817.

Liederman, E. M., & Morefield, C. S. (2003). Web messaging: A new tool for patient-physician communication. *Journal of the American Medical Informatics Association, 10*(3), 260-270. doi: 10.1197/jamia.M1259

Mandl, K. D., & Kohane, I. S. (1999). Healthconnect: Clinical grade patient-physician communication. Paper presented at the *AMIA (American Medical Informatics Association.) Proceedings: Annual Symposium.AMIA Symposium 1999,* 849-853.

Mandl, K. D., Kohane, I. S., & Brandt, A. M. (1998). Electronic patient-physician communication: Problems and promise. *Annals of Internal Medicine, 129*(6), 495-500.

McKibbon, K. A., Lokker, C., Handler, S. M., Dolovich, L. R., Holbrook, A. M., O'Reilly, D., et al. (2011). *Enabling medication management through health information technology.* (Evidence Reports/Technology Assessments No. 11-E008-EF). Rockville, MD: Agency for Healthcare Research and Quality.

Mercuri, R. T. (2004, The HIPAA-potamus in health care data security. *Communications of the ACM, 47,* 25-28.

Microsoft Health Vault. (2012). *What is HealthVault?* Retrieved August 19, 2012, from http://msdn.microsoft.com/en-us/healthvault/jj128027

Ministry of Health British Columbia. (2012a). *eHealth overview.* Retrieved October 4, 2012, from http://www.health.gov.bc.ca/ehealth/pdf/eHealthBrochure.pdf

Ministry of Health British Columbia. (2012b). *Electronic health record (EHR).* Retrieved October 04, 2012, from http://www.health.gov.bc.ca/ehealth/ehr.html

Moya, K. M. (2011). *What can we learn from the rest of the world? A look at international electronic health record best practices.* Retrieved August 10, 2011, from http://www.moyak.com/papers/best-practices-ehr.html

MySQL. (2012). *About MySQL.* Retrieved August 27, 2012, from http://www.mysql.com/about/

Neilson, J. (2012). *Current issues in web usability.* Retrieved August 26, 2012, from http://www.useit.com/alertbox/

Nieuwlaat, R., Connolly, S., Mackay, J., Weise-Kelly, L., Navarro, T., Wilczynski, N., et al. (2011) Computerized clinical decision support systems for therapeutic drug monitoring and dosing: A decision-maker-researcher partnership systematic review. *Implementation Science, 6*(1), 90.

Office of Auditor General of Ontario. (2009). *Ontario's electronic health records initiative.* (Special Report). Toronto, ON: Queen's Printer for Ontario.

Protti, D., & Johansen, I. (2010) Widespread adoption of information technology in primary care physician offices in Denmark: A case study. *The Commonwealth Fund: Issue Brief, 80*, 1-14.

reCAPTCHA. (2012). *What is reCAPTCHA?* Retrieved August 23, 2012, from http://www.google.com/recaptcha/learnmore

Rescorla, E. (2001). Introduction to SSL. *SSL and TLS, Designing And Building Secure Systems*. Upper Saddle River, NJ: Addison-Wesley.

Shekelle, P. G., Morton, S. C., & Keeler, E. B. (2006). *Costs and benefits of health information technology.* (Evidence Report/Technology Assessment No. 132). United States: AHRQ: Agency For Healthcare Research and Quality.

Shiffman, R. N., Liaw, Y., Brandt, C. A., & Corb, G. J. (1999). Computer-based guideline implementation systems: A systematic review of functionality and effectiveness. *Journal of the American Medical Informatics Association, 6*(2), 104-114.

Shortliffe, E. H. (2005). Strategic action in health information technology: Why the obvious has taken so long. *Health Affairs (Project Hope), 24*(5), 1222-1233.

The Canadian Medical Protective Association. (2012). *CMPA - electronic records handbook* Retrieved August 19, 2012, from http://www.cmpa-acpm.ca/cmpapd04/docs/submissions_papers/com_electronic_records_handbook-e.cfm

The Economist Intelligence Unit. (2012). *Denmark: Electronic patient records.* Retrieved August 15, 2012, from http://www.reforminghealthcare.eu/economist-report/some-roads-ahead-innovative-approaches-in-five-west-european-countries/denmark-electronic-patient-records

Venkatesh, V., Morris, M. G., Gordon B. Davis, & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. *MIS Quarterly, 27*(3), 425-478.

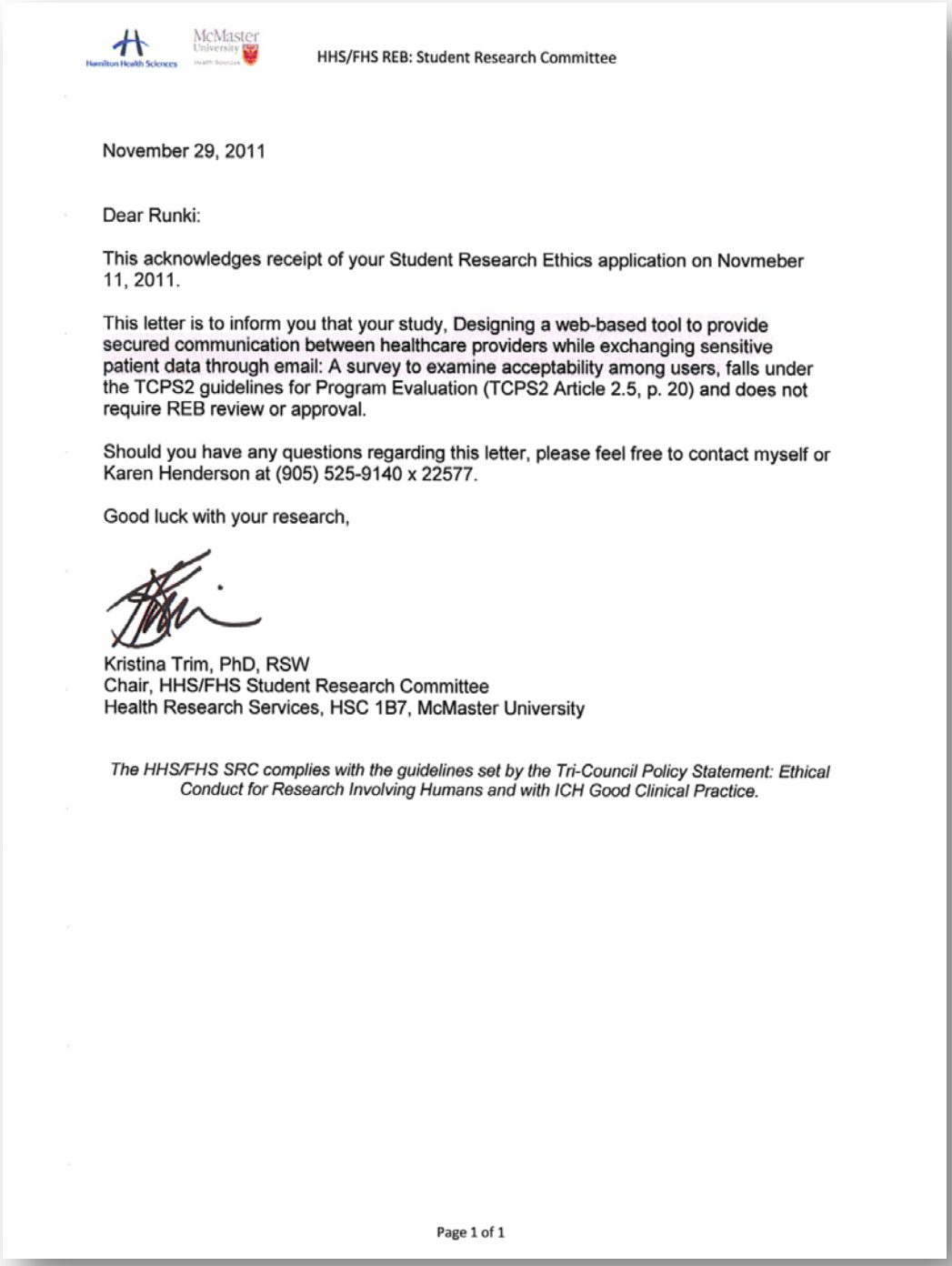
Walker, J., Pan, E., Johnston, D., Adler-Milstein, J., Bates, D. W., & Middleton, B. (2005). The value of health care information exchange and interoperability. *Health Affairs (Project Hope), Suppl Web Exclusives*, W5-10-W5-18.

Webster, P. C. (2012). Nothing cutting edge about Canadian ehealth strategy, critics say. *CMAJ, 184*(1), E35-6.

Yaping, Y., & Weiqi, L. (2001). Design and implementation of SSL based secure transmission system. *Journal of Beijing University of Aeronautics and Astronautics*, (4), 469-473.

Ye, J., Rust, G., Fry-Johnson, Y., & Strothers, H. (2010). E-mail in patient-provider communication: A systematic review. *Patient Education and Counseling, 80*(2), 266-273.

APPENDIX A – Letter from Research Ethics Board



Hamilton Health Sciences McMaster University

HHS/FHS REB: Student Research Committee

November 29, 2011

Dear Runki:

This acknowledges receipt of your Student Research Ethics application on Novmeber 11, 2011.

This letter is to inform you that your study, Designing a web-based tool to provide secured communication between healthcare providers while exchanging sensitive patient data through email: A survey to examine acceptability among users, falls under the TCPS2 guidelines for Program Evaluation (TCPS2 Article 2.5, p. 20) and does not require REB review or approval.

Should you have any questions regarding this letter, please feel free to contact myself or Karen Henderson at (905) 525-9140 x 22577.

Good luck with your research,

Kristina Trim, PhD, RSW
Chair, HHS/FHS Student Research Committee
Health Research Services, HSC 1B7, McMaster University

The HHS/FHS SRC complies with the guidelines set by the Tri-Council Policy Statement: Ethical Conduct for Research Involving Humans and with ICH Good Clinical Practice.

Page 1 of 1

APPENDIX B – User Guideline for ST-SecRx

INSTRUCTION FOR USING ST-SecRx

Title

Designing Prototype of a Web-Based System to Provide Secured Communication between Healthcare Providers While Exchanging Sensitive Patient Data through Email: A Survey to Examine Acceptability among Users

INVESTIGATORS:

Local Principal Investigator:

Dr. Ann McKibbon, Ph.D.
Associate Professor
Clinical Epidemiology & Biostatistics,
McMaster University
Hamilton, ON L8S 4L8
Phone: 905-525-9140 X 22803; Fax: 905-546-0401
E-mail: mckib@mcmaster.ca

Co-Investigators:

Runki Basu
Graduate Student
McMaster University
Hamilton, ON L8S 4L8
Phone: 416-875-1546
E-mail: basur3@mcmaster.ca

Dr. Tapas Mondal, **MBBS, MD, MRCPCH, FRCPC**
Associate Professor, Pediatrics,
Department of Pediatrics
McMaster University
Hamilton, ON
Phone: 905-521-2100 X 75242
E-mail: **mondalt@mcmaster.ca**

ST-SecRX

ST-SecRx is a prototype of a web-based system for secured communication between healthcare providers while exchanging sensitive patient data through email. I have designed the system for my Master's Thesis.

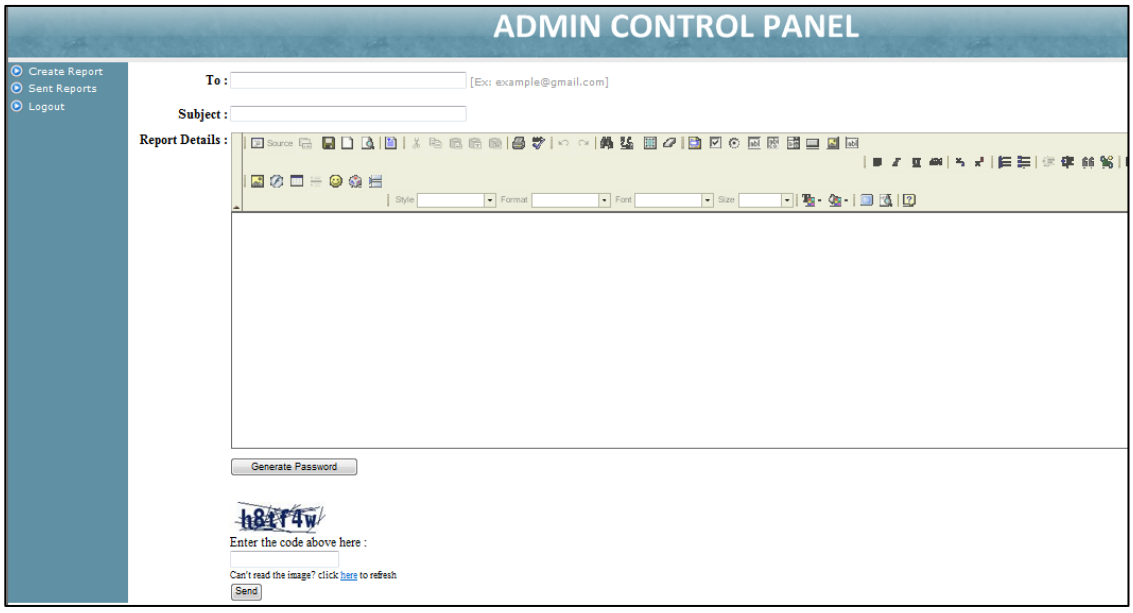
Step-by-Step Instruction To Use ST-SecRx

In order to check the solution you have to go through the following steps:

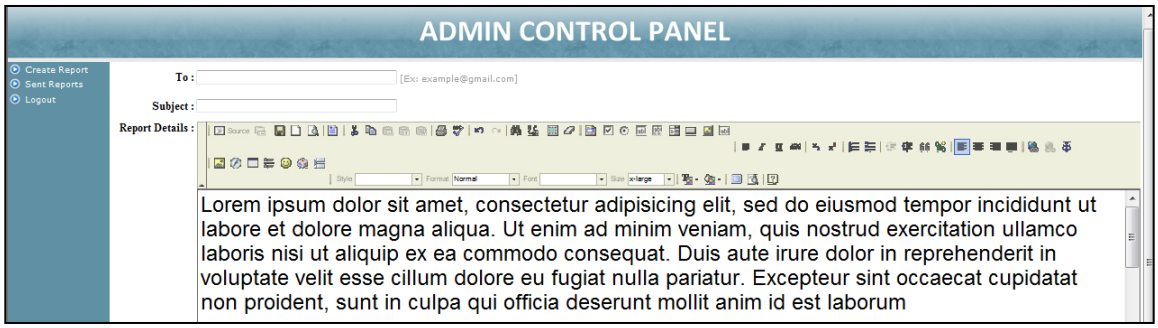
1) Click on the URL: http://www.glendoncg.com/prs/login.php

2) It will open a browser with a Login screen. Enter user name and password.
   User Name: admin
   Password: admin

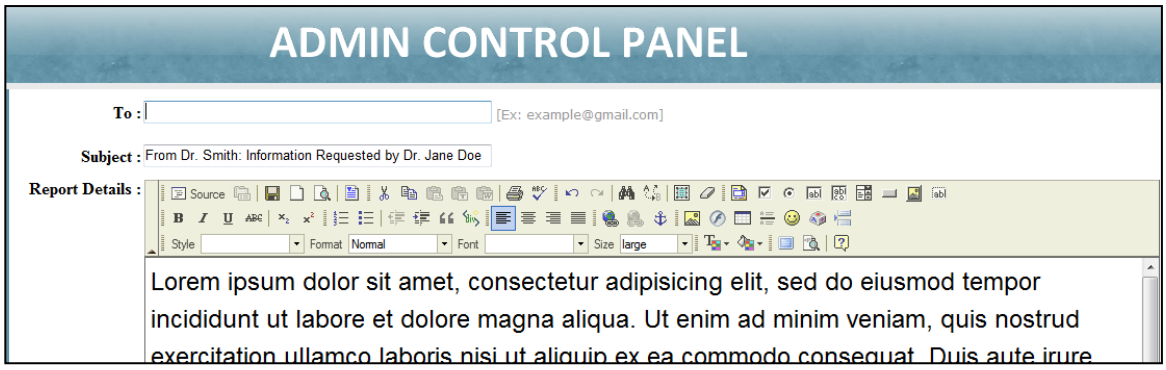
3) Once you log in you will find a screen with a text editor.



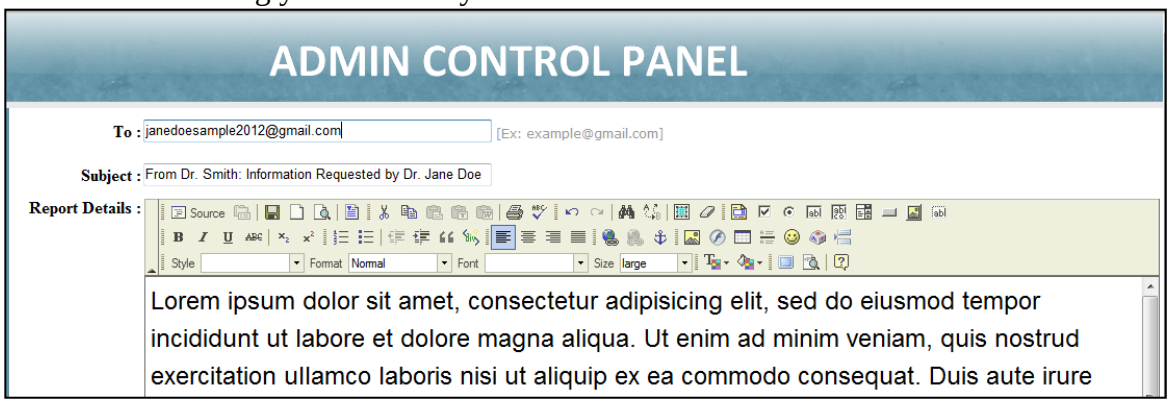
4) You can copy information from other files or enter information in this textbox called "Report Details".



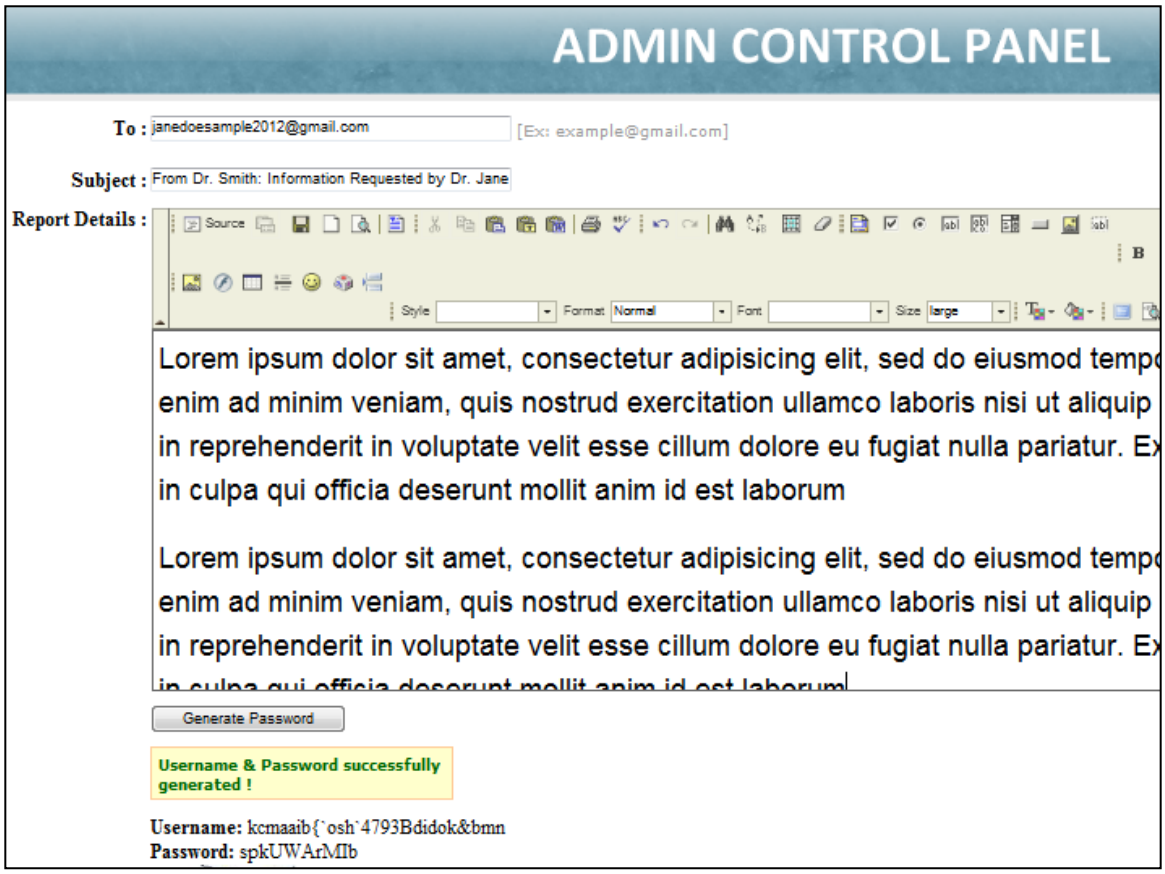
5) Then type an appropriate subject matter. Subject matter should be such that it cannot be used as an identifier against any patient. For Example, you can type in "From Dr. Smith: Information Requested by Dr. Jane Doe" but NOT "Information of Patient Baby John".



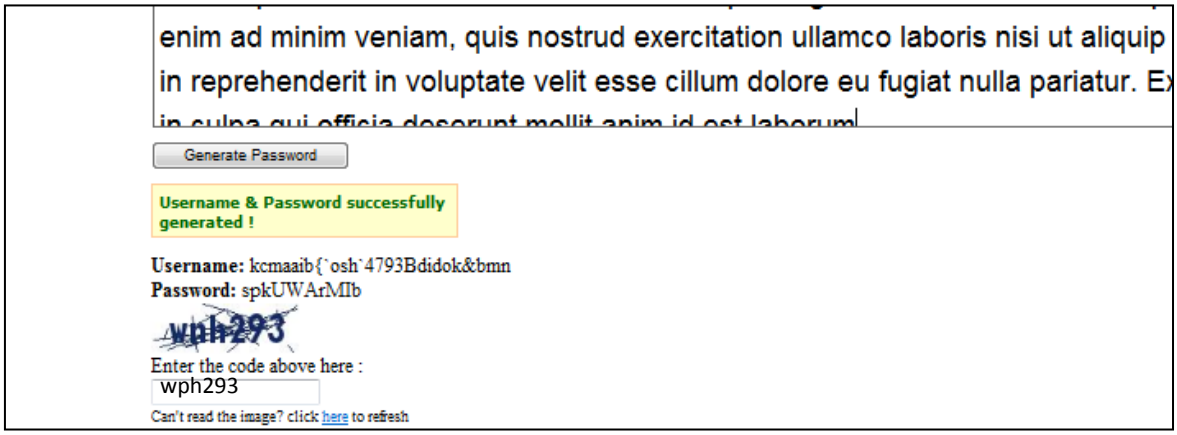
6) The next step for you would be to type in the email of the recipient at the "To" field. For test checking you can enter your own email.



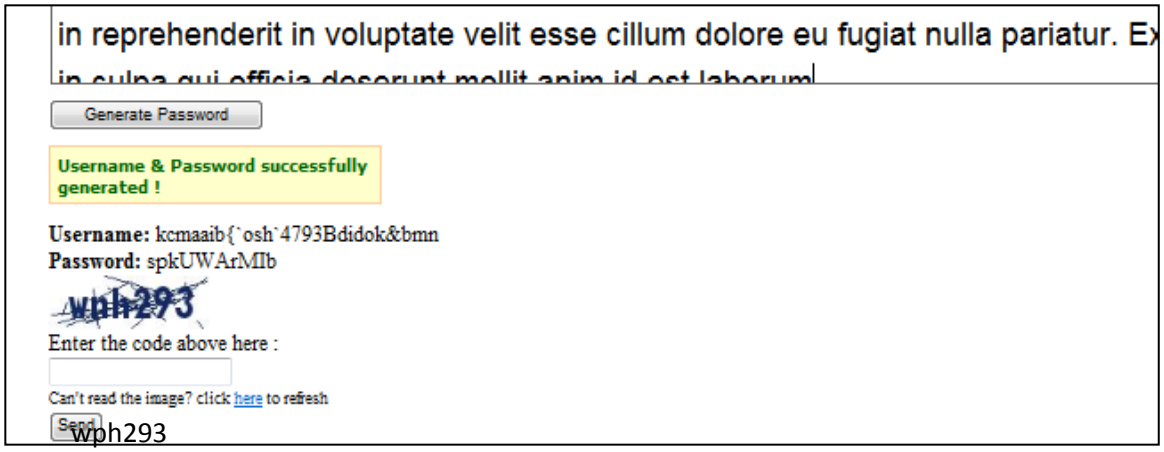
7) You then have to click on button called "Generate Password" at the bottom of the screen to generate a User Name and Password for the recipient. *(You do not have copy the user name and password. It will automatically be sent to the recipient's email.)*



8) Then you have to enter the CAPTCHA words in the textbox "Enter the code above here:"



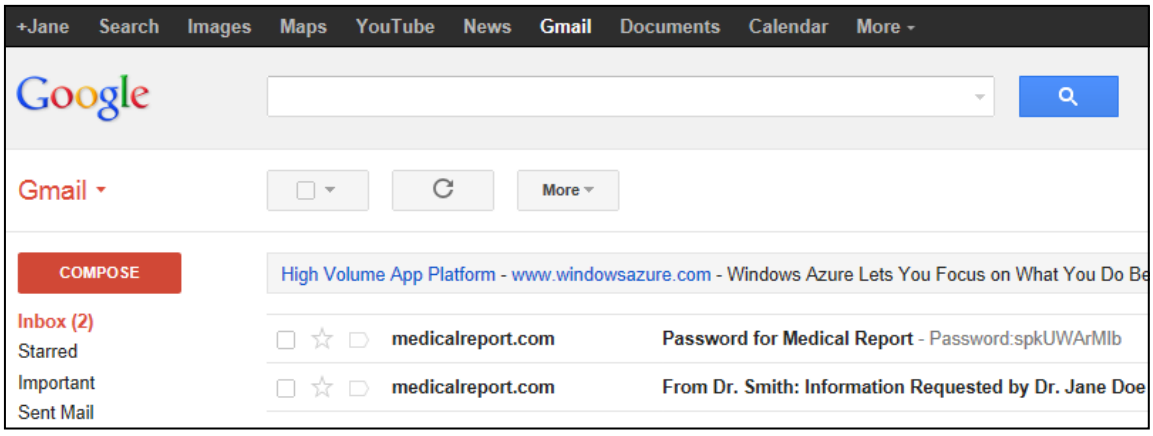
9) Finally click the send button at the bottom of the screen.



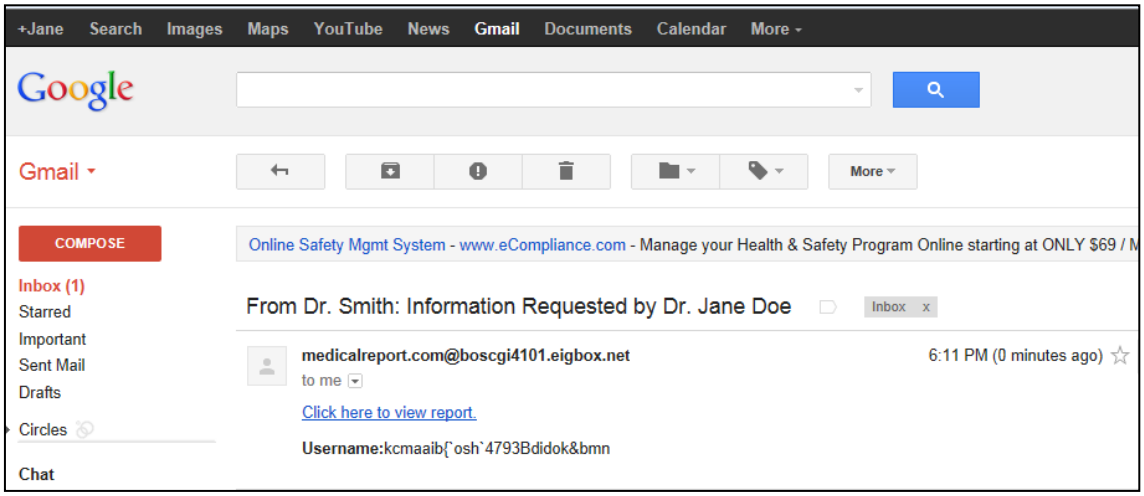
10) Once sent, the ST-SecRx will generate a link with encrypted parameter value that does not link itself to any patient data.

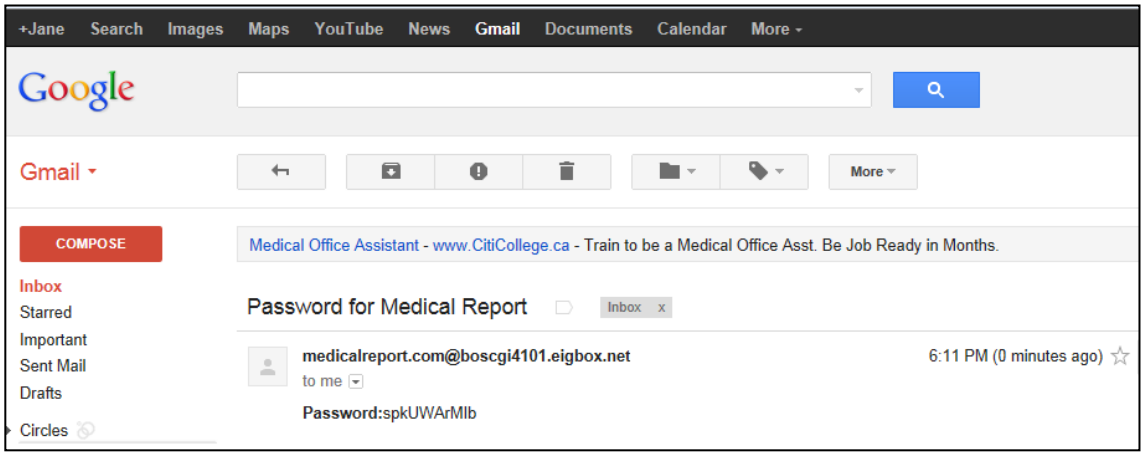
11) After sending you can send another report. In order to do so you have to click on the "Create Report" on the left menu bar in the Admin Control Panel. This will again open up the Text Editor and create a new report for another recipient. Otherwise, you can just logout from the system.

12) Recipient receives two emails one with the encrypted link and username. The other with the password.

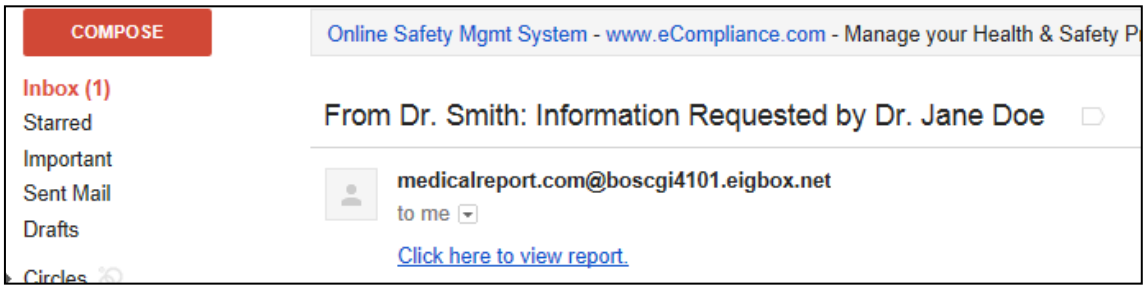


13) The two emails received by the Recipient will contain the following information.

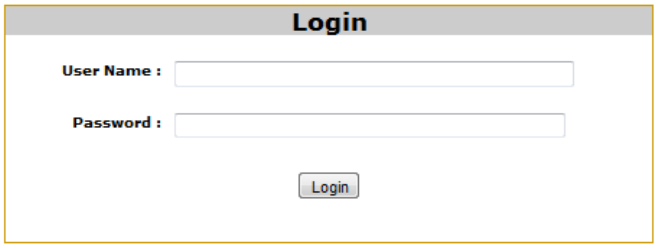




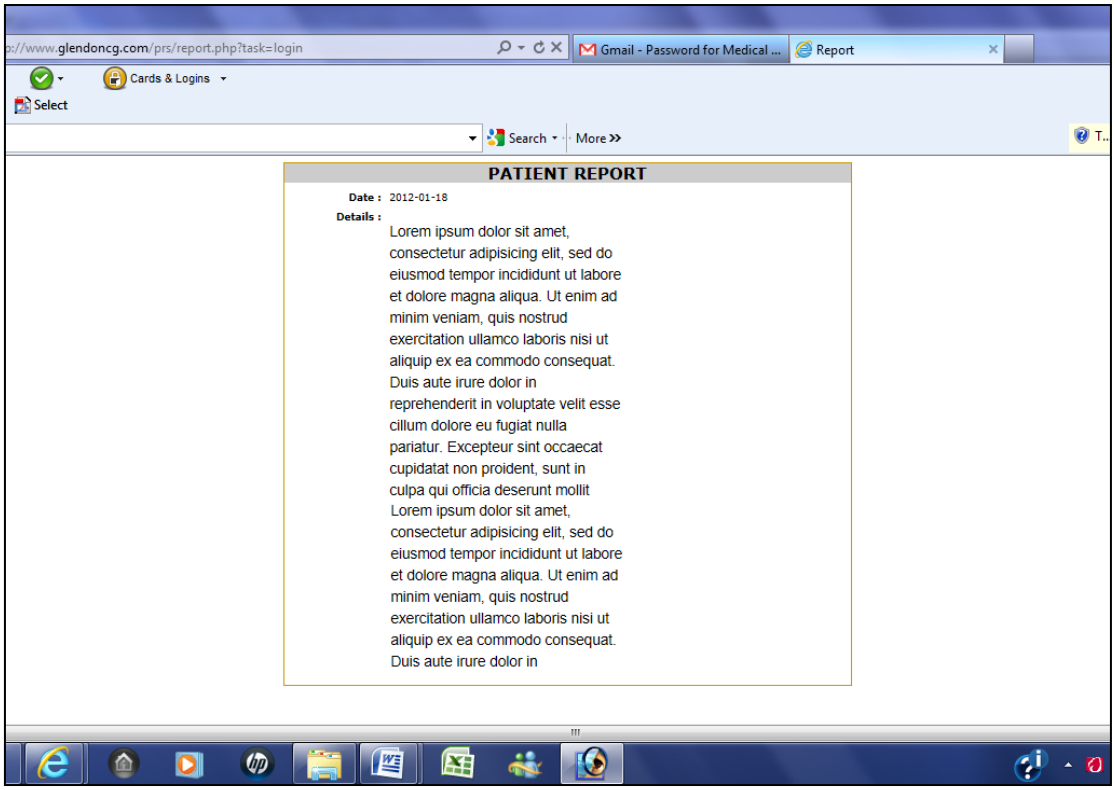
14) Recipient will have to click on the link to view patient data.



15) At the prompt, a login screen will open and the Recipient will have to enter the user name and password received in the two emails.



16) The data will be downloaded into target computer through an encrypted and secure (https) method that is safe. And the Patient Report will be displayed as given below.



APPENDIX C – Survey Questionnaire

QUESTIONNAIRE

Designing Prototype of a Web-Based System to Provide Secured Communication between Healthcare Providers While Exchanging Sensitive Patient Data through Email: A Survey to Examine Acceptability among Users

INVESTIGATORS:

Local Principal Investigator:

Dr. Ann McKibbon, Ph.D.
Associate Professor
Clinical Epidemiology & Biostatistics,
McMaster University
Hamilton, ON L8S 4L8
Phone: 905-525-9140 X 22803: Fax: 905-546-0401
E-mail: mckib@mcmaster.ca

Co-Investigators:

Runki Basu
Graduate Student
McMaster University
Hamilton, ON L8S 4L8
Phone: 416-875-1546
E-mail: basur3@mcmaster.ca

Dr. Tapas Mondal, **MBBS, MD, MRCPCH, FRCPC**
Associate Professor, Pediatrics,
Department of Pediatrics
McMaster University
Hamilton, ON
Phone: 905-521-2100 X 75242
E-mail: mondalt@mcmaster.ca

Instructions

Please base your responses to the following questions on your current perceptions of using ST-SecRx for secure communication between healthcare providers while exchanging sensitive patient data through email.

GENERAL QUESTIONS

1. **Please select your age range.**

- ◯<30
- ◯30 - 39
- ◯40 – 49
- ◯50 – 60
- ◯>60

2. **Please select your gender.**

- ◯Female
- ◯Male

3. **Please specify your occupation:**

- ◯Primary Care Physicians
- ◯Specialists
- ◯Other Physicians, Specify _____

CURRENT FORM OF EMAIL USED FOR PATIENT DATA EXCHANGE

4. **Do you use email provided by your organistaion for exchanging sensitive patient data?**

- ◯Yes
- ◯No

5. **Do you use an email service or a web messaging service that lets you send sensitive patient data securely between registered users?**

- ◯Yes
- ◯No

If you selected "Yes" to Question #5, please provide the name of the email service provider / solution used:_____

THE FOLLOWING QUESTIONS MUST BE ANSWERED AFTER YOU HAVE USED ST-SecX.

FACTORS THAT WOULD FACILATE YOUR USE OF ST-SecRx

6. **Please indicate whether you agree that the following factors are important for using ST-SecRx for sending and receiving confidential and secure patient information. Answer according to whether you : strongly agree (5), moderately agree (4), neither agree nor disagree (3), moderately disagree (2), strongly disagree (1)**

Ease of Use	1	2	3	4	5
Not having to use an email different from the email provided by your employer for exchanging sensitive patient data.	1	2	3	4	5
Not having to create / reset and remember a New Password Every 3/6 months for using an email different from the email provided by your organization .	1	2	3	4	5
My confidence/ sense of security that my data transfer complies with regulations related to privacy and security of patient information.	1	2	3	4	5

PERCEIVED USEFULNESS OF ST-SecRx

7. **Please select the response that best represents your level of agreement with the following statements. Answer according to whether you: strongly agree (5), moderately agree (4), neither agree nor disagree (3), moderately disagree (2), strongly disagree (1)**

ST-SecRx is more secure compared to previously used methods of patient data exchange through email.	1	2	3	4	5
ST-SecRx is easy to use compared to previously used methods of patient data exchange through email.	1	2	3	4	5

BEHAVIOURAL INTENTION TO USE ST-SecRx

8. Transfer of patient data may be done for consultation on treatments, transfer of the patient to other facilities, requests for consultation or advice, reporting back on consultations, general communication, etc. In view of this, **please select the response that best represents your level of agreement with the following statements. Answer according to whether you: strongly agree (5), moderately agree (4), neither agree nor disagree (3), moderately disagree (2), strongly disagree (1)**

If ST-SecRx is available to me, I intend to take advantage of it when exchanging patient data.	1	2	3	4	5
If ST-SecRx is available to me, I am likely to use it more often than other means of patient data exchange through email.	1	2	3	4	5
If ST-SecRx is available to me, I intend to use this as the ONLY means of exchanging patient data through email.	1	2	3	4	5
If ST-SecRx is available to me, I am likely to use ONLY this as means of patient data exchange through email.	1	2	3	4	5
Use of ST-SecRx would enhance my effectiveness in managing my patients' health care.	1	2	3	4	5
Use of ST-SecRx would reduce duplication of requests for diagnostic tests between different healthcare providers.	1	2	3	4	5

9. Which feature of ST-SecRx did you like the most?

_____

10. Which feature of ST-SecRx did you like the least?

_____

11. Would you be willing to pay for the ST-SecRx service?
    - ◯Yes
    - ◯No

12. If you answered "Yes" to Question 11, how much per month or per year are your willing to pay?

    _____

13. ☐ Please check if you would like a copy of the final report.

Thank you for completing this questionnaire.

APPENDIX D – Consent Form

INFORMATION/CONSENT FORM FOR PHYSICIANS

Title

Designing Prototype of a Web-Based System to Provide Secured Communication between Healthcare Providers While Exchanging Sensitive Patient Data through Email: A Survey to Examine Acceptability among Users

INVESTIGATORS:

Local Principal Investigator:

Dr. Ann McKibbon, Ph.D.
Associate Professor
Clinical Epidemiology & Biostatistics,
McMaster University
Hamilton, ON L8S 4L8
Phone: 905-525-9140 X 22803; Fax: 905-546-0401
E-mail: mckib@mcmaster.ca

Co-Investigators:

Runki Basu
Graduate Student
McMaster University
Hamilton, ON L8S 4L8
Phone: 416-875-1546
E-mail: basur3@mcmaster.ca

Dr. Tapas Mondal, **MBBS, MD, MRCPCH, FRCPC**
Associate Professor, Pediatrics,
Department of Pediatrics
McMaster University
Hamilton, ON
Phone: 905-521-2100 X 75242
E-mail: **mondalt@mcmaster.ca**

Invitation to Participate in Research

I am a graduate student of M.Sc., eHealth working on designing a prototype of a web-based tool called ST-SecRx to provide secured communication between healthcare providers while exchanging sensitive patient data through email. I am working under the guidance of Dr. Ann McKibbon. My co-investigator is Dr. Tapas Mondal.

I invite you to participate in this study, and I am interested in your opinion about using ST-SecRx designed and developed by us.

Purpose of this Study

The Department of Paediatrics at McMaster Children's Hospital has been experiencing a problem while exchanging patient information within and outside the organization. Often, the physicians at the department refer patients to outside care facilities, particularly to children's hospitals in Toronto. Common practice with the physicians in the past was to send relevant patient data to the attending physicians at these hospitals through email. This practice has been stopped at McMaster Children's Hospital after having been flagged by privacy audit as violation of patient privacy.

Unrestricted use of patient data through email is a clear violation of the patients' privacy and security. We have developed a prototype of a web-based solution called ST-SecRx, by using data encryption techniques that will comply with all relevant privacy regulations. Our approach does not require transmission of any patient data directly through email. Instead, it involves storing encrypted patient data in a database over the Internet. The system generates a link with encrypted parameter value that does not link itself to any patient data. This URL link is emailed by the physicians at McMaster Children's Hospital to the recipient via regular email. Subsequently, the data will be reviewed by the target physicians by clicking on a hyperlink. The hyperlink does not carry any identifier that can be linked to any patients.

The purpose of the survey is to examine acceptability of the prototype ST-SecRx.

I believe that the findings from this study will help in secure communication among clinicians while complying with privacy regulations with an aim to extend its use in future by other healthcare professionals exchanging sensitive clinical data.

Number of Participants

I will conduct a survey with a maximum of 30 Physicians by using a Questionnaire. Any Physician located in Hamilton and Greater Toronto Area who uses email can participate in the survey.

Procedures involved in the Research

The Study will be conducted in two steps after receiving formal consent from you:

Step 1: I will send you an email with a Universal Recourse Locator (URL) to use the prototype of the web-based tool ST-SecRx using dummy data. The email will also have detailed instruction on how to use ST-SecRx.

a. When you click on the URL it will open a browser with a text editor. You can enter information using the text editor.
b. You will then be required to click on button to generate a User Id and Password for the recipient.
c. The next step for you would be to type recipient's email id and click the send button.
d. Once sent, the ST-SecRx will generate a link with encrypted parameter value that does not link itself to any patient data.
e. The recipient receives two emails one with the encrypted link and user id. And the other with the password.
f. Recipient will have to click on the link to view patient data. At the prompt, it will ask for the user id and password to display the information. The data will be downloaded into target computer through an encrypted and secure (https) method that is safe.

Step 2: Subsequently, I will conduct a survey in the form a questionnaire which will be available both online and as printed document. You can participate in the Survey in any of the following two ways:

Option 1: A face-to-face interview with you to determine your acceptability to use ST-SecRx. I intend to do this using a Questionnaire.

a. Time required: about 15 minutes

b. Place of interview: Your office or a place of your choice

c. Mode of taking Notes: Handwritten notes

Option 2: The survey will be available online for you to participate.

a. Time required: about 10 minutes

Your data will be used for my Master's Thesis.

Risks

It is unlikely that your participation in this study will cause any discomfort or harm. Some of the questions may cause you to reflect on issues or decisions that may be a source of reflection for you. Any responses you provide will be treated confidentially by the researchers named above.

Benefits

This study is not meant to be of benefit to individual participants; however we believe that the findings from this study will be helpful for those who design and implement secure communication for clinicians while complying with privacy regulations. If successful we aim to extend its use to other healthcare professionals exchanging sensitive clinical data through emails.

Compensation

You will not be paid to be in this study, but we do appreciate your participation.

Cost to Participants

We do not anticipate any cost to you for participating in this study. Your time will be approximately half an hour to review the emails we send you and answer the short questionnaire.

Confidentiality

Participation in this study is voluntary and all information collected will be stored securely and kept in strict confidence. Only the investigators named above will have access to the data. You will not be identified individually in any reports or analyses resulting from this research project. All data storage will be done using data with no identifiers.

Withdrawal

This is a one-time participation. You may terminate your participation in this interview or the online survey at any time. If you choose to terminate your participation in the interview or the online survey, any data you have provided will be destroyed unless you indicate otherwise.

Contact Information

If you have any questions or concerns regarding this study, please contact the principal investigators named above.

Consent

I have read the preceding information thoroughly. I have had an opportunity to ask questions and all of my questions have been answered to my satisfaction. I agree to participate in this study. I understand that I will receive a signed copy of this form.

Name	Signature	Date

Person obtaining consent:

I have discussed this study in detail with the participant. I believe the participant understands what is involved in this study.

Name, Role in Study	Signature	Date

If you have any questions about your rights as a research participant, please call The Office of the Chair, HHS/FHS REB at 905.525.2100 x 42013.

APPENDIX E – Email to Physicians

Sample Email #1 To Physicians

Dear Dr._____,
I am a graduate student of M.Sc., eHealth Program at McMaster University. For a research project, I have designed a prototype of a web-based tool called ST-SecRx to provide secured communication between healthcare providers while exchanging sensitive patient data through email.
I am working under the guidance of Dr. Ann McKibbon of McMaster University My co-investigator is Dr. Tapas Mondal of McMaster University.
I would like to invite you to participate in a study to examine the acceptability of the prototype ST-SecRx.
I have attached a step-by-step instructions guide to help you walk through the software.

There will be two steps involved in the survey. Here is what is needed:

1) First Step: (Will take about 5 to 10 minutes)
Please look through the attached instructions document and review the online software:
http://www.glendoncg.com/prs/login.php
User Name: admin
Password: admin

2) Second Step: (Will take about 3 to 5 Minutes)
After you have used ST-SecRx, please take the brief online survey to answer 13 questions.
http://limesurvey.degroote.mcmaster.ca/index.php?sid=38825&lang=en
Alternatively, you can also complete the survey by responding to the attached questionnaire and consent form and email it to me.

Participation in this study is voluntary and all information collected will be stored securely and kept in strict confidence. Only the investigators involved in the study will have access to the data. You will not be identified individually in any reports or analyses resulting from this research project. All data storage will be done using data with no identifiers.

If would like to get a copy of the Final Report please email me and let me know.

At any point of time if you have any questions, please feel free to call me at 416-XXX-XXXX.

I look forward to your participation in the survey and get your opinion on the subject.

Thanks,

Runki Basu

Sample Email #2 To Physicians

Dear Dr. _____,

I am a graduate student of M.Sc., eHealth Program at McMaster University working under the guidance of Dr. Ann Mckibbon.

For my Master's thesis I have designed a prototype of a web-based tool called ST-SecRx to provide secured communication between physicians while exchanging sensitive patient data through email. My co-investigator is Dr. Tapas Mondal of McMaster University.

I would like to invite you to participate in a study to examine the acceptability of the prototype ST-SecRx.

Would appreciate if you could please meet with at a time of your convenience for 10-15 minutes, then I can come and give a demo of the online software and get your feedback for the survey.

Thanks,

Runki Basu

Sample Email #3 To Physicians

Dear Dr._____,
Thank you very much for agreeing to participate in a study for my Master's thesis for M.Sc. eHealth Program at McMaster University.
As I mentioned over the phone, I have designed a prototype of a web-based tool called ST-SecRx to provide secured communication between healthcare providers while exchanging sensitive patient data through email.
I am working under the guidance of Dr. Ann McKibbon of McMaster University My co-investigator is Dr. Tapas Mondal of McMaster University.
I would like to invite you to participate in a study to examine the acceptability of the prototype ST-SecRx.
I have attached a step-by-step instructions guide to help you walk through the software.

There will be two steps involved in the survey. Here is what is needed:

1) First Step: (Will take about 5 minutes)
Please look through the attached instructions document and review the online software:
http://www.glendoncg.com/prs/login.php
User Name: admin
Password: admin

2) Second Step: (Will take about 5 Minutes)
After you have used ST-SecRx, please take the brief online survey to answer 13 questions.
http://limesurvey.degroote.mcmaster.ca/index.php?sid=38825&lang=en
Alternatively, you can also complete the survey by responding to the attached questionnaire and consent form and email it to me.

Participation in this study is voluntary and all information collected will be stored securely and kept in strict confidence. Only the investigators involved in the study will have access to the data. You will not be identified individually in any reports or analyses resulting from this research project. All data storage will be done using data with no identifiers.

If would like to get a copy of the Final Report please email me and let me know.

At any point of time if you have any questions, please feel free to call me at 416-XXX-XXXX.

I look forward to your participation in the survey and get your opinion on the subject.

Thanks,

Runki Basu

Sample Email #4 To Physicians

Runki Basu is a graduate student of M.Sc., eHealth Program at McMaster University. For a research project, she has designed a prototype of a web-based tool called ST-SecRx to provide secured communication between physicians while exchanging sensitive patient data through email.

She is working under the guidance of Dr. Ann McKibbon of McMaster University and her co-investigator is Dr. Tapas Mondal of McMaster University.

She would like to invite you to participate in a study to examine the acceptability of the prototype ST-SecRx.

Attached is a step-by-step instructions guide to help you walk through the software.
There will be two steps involved in the survey. Here is what is needed:

1) First Step: (Will take about 10 minutes)
Please look through the attached instructions document and review the online software:
http://www.glendoncg.com/prs/login.php
User Name: admin
Password: admin

2) Second Step: (Will take about 3 to 5 Minutes)
After you have used ST-SecRx, please take the brief online survey to answer 13 questions.
http://limesurvey.degroote.mcmaster.ca/index.php?sid=38825&lang=en

Runki will be available to give a demo of the software at a time of your convenience and get your feedback. She can be contacted at runki.basu@gmail.com .

Participation in this study is voluntary and all information collected will be stored securely and kept in strict confidence. Only the investigators involved in the study will have access to the data. You will not be identified individually in any reports or analyses resulting from this research project. All data storage will be done using data with no identifiers.

Sample Email #5 To Physicians

Dear Dr. _____,

I am a graduate student of M.Sc., eHealth Program atMcMaster University working under the guidance of Dr. Ann Mckibbon.

For my Master's thesis I have designed a prototype ofa web-based tool called ST-SecRx to provide secured communication betweenphysicians while exchanging sensitive patient data through email. My co-investigator is Dr. Tapas Mondal of McMaster University.

I would like to invite you to participate in a study to examine the acceptability of the prototype ST-SecRx.

Would appreciate if you could please meet with me at a time of your convenience for 10-15 minutes, then I can come and give a demo of the online software and get your feedback for the survey.

Alternatively, you could participate by reviewing the software by following the attached a step-by-step instructions guide to help you walk through the software and then participate in the survey.

There are two steps involved in the survey.
1) First Step: (Will take about 5 to 10 minutes)
Please look through the attached instructions document and review the online software:
http://www.glendoncg.com/prs/login.php
User Name: admin
Password: admin

2) Second Step: (Will take about 3 to 5 Minutes)
After you have used ST-SecRx, please take the brief online survey to answer 13 questions.
http://limesurvey.degroote.mcmaster.ca/index.php?sid=38825&lang=en

Participation in this study is voluntary and all information collected will be stored securely and kept in strict confidence. Only the investigators involved in the study will have access to the data. You will not be identified individually in any reports or analyses resulting fromthis research project. All data storage will be done using data with no identifiers.

I will use the data collected from the Survey for myMaster's Thesis.
I look forward to your participation in the survey and get your opinion on the subject.
Thanks,
Runki Basu

APPENDIX F – Additional Tables

Table 14: Analysis of " Using Email Provided by Organization" by Sex, Age and Occupation

	Sample Size	Yes	No	Did Not Answer
All Respondents	n=19	11 (57.9%)	7 (36.8%)	1 (5.3%)
Sex				
Men	n=15	9 (60%)	6 (40%)	-
Women	n= 3	2 (66.7%)	1 (33.3%)	-
Sex Not Disclosed	n= 1	-	-	1 (100%)
Age Group				
<30 Years	n=3	2 (66.7%)	1 (33.3%)	-
30-39 Years	n=4	3 (75%)	1 (25%)	-
40-49 Years	n=8	4 (50%)	3 (37.5%)	1 (12.5%)
50-59 Years	n=3	2 (66.7%)	1 (33.3%)	-
>60 Years	n=1	-	1 (100%)	-
Occupation				
Primary Care Physicians	n=7	3 (42.9%)	4 (57.1%)	-
Specialists	n=7	5 (71.4 %)	2 (28.6%)	-
Other Physicians	n=4	3 (75%)	1 (25%)	-
Occupation Not Disclosed	n=1	-	-	1 (100%)

*:Using Email Provided by Organization for Exchanging Sensitive Patient Data

Table 15: Analysis of "Using Email or Web Messaging Service"* by Sex, Age and Occupation

	Sample Size	Yes	No	Did Not Answer
All Respondents	n=19	2 (10.5%)	16 (84.2%)	1 (5.3%)
Sex				
Men	n=15	2 (13.3%)	13 (86.7%)	-
Women	n= 3	-	3 (100%)	-
Sex Not Disclosed	n= 1	-	-	1 (100%)
Age Group				
<30 Years	n=3	1 (33.3%)	2 (66.7%)	-
30-39 Years	n=4	-	4 (100%)	-
40-49 Years	n=8	1 (12.5%)	6 (75%)	1 (12.5%)
50-59 Years	n=3	-	3 (100%)	-
>60 Years	n=1	-	1 (100%)	-
Occupation				
Primary Care Physicians	n=7	1 (14.3%)	6 (85.7%)	-
Specialists	n=7	-	7 (100%)	-
Other Physicians	n=4	1 (25%)	4 (75%)	-
Occupation Not Disclosed	n=1	-	-	1 (100%)

* Using Email or Web Messaging Service to Send Sensitive Patient Data Securely Between Registered Users

Table 16: Analysis of Factor "Ease of Use" by Age, Sex and Occupation

Factor: Ease of Use	Sample Size	Agree*	Neither Agree Nor Disagree	Disagree**	No Answer
All Respondents	n=19	15 (79%)	1 (5.3%)	1 (5.3%)	2 (10.5%)
Sex					
Men	n=15	13 (86.7%)	-	1 (6.7%)	1 (6.7%)
Women	n= 3	2 (66.7%)	1 (33.3%)	-	-
Sex Not Disclosed	n= 1	-	-	-	1 (100%)
Age Group					
<30 Years	n=3	3 (100%)	-	-	-
30-39 Years	n=4	3 (75%)	-	1 (25%)	-
40-49 Years	n=8	7 (87.5%)	-	-	1(12.5%)
50-59 Years	n=3	2 (66.7%)	1 (33.3%)	-	-
>60 Years	n=1	-	-	-	1 (100%)
Occupation					
Primary Care Physicians	n=7	7 (100%)	-	-	-
Specialists	n=7	4 (57.1%)	1 (14.3%)	1 (14.3%)	1 (14.3%)
Other Physicians	n=4	4 (100%)	-	-	-
Occupation Not Disclosed	n=1				1 (100%)

* Agree = Strongly Agree or Moderately Agree

** Disagree = Strongly Disagree or Moderately Disagree

Table 17: Analysis of Factor "Do not have to use an email different from the one provided by employer" by Sex, Age and Occupation

Factor: Not having to use an email different from the email provided by your employer for exchanging sensitive patient data	Sample Size	Agree*	Neither Agree Nor Disagree	Disagree**	No Answer
All Respondents	n=19	14 (73.7%)	2 (10.5%)	1 (5.3%)	2 (10.5%)
Sex					
Men	n=15	11 (73.3%)	2 (13.3%)	1 (6.7%)	1 (6.7%)
Women	n= 3	3 (100%)	-	-	-
Sex Not Disclosed	n= 1	-	-	-	1 (100%)
Age Group					
<30 Years	n=3	3 (100%)	-	-	-
30-39 Years	n=4	3 (75%)	-	1 (25%)	-
40-49 Years	n=8	6 (75%)	1 (12.5%)	-	1(12.5%)
50-59 Years	n=3	2 (66.7%)	1 (33.3%)	-	-
>60 Years	n=1	-	-	-	1 (100%)
Occupation					
Primary Care Physicians	n=7	7 (100%)	-	-	-
Specialists	n=7	3 (42.9%)	2(28.6%)	1 (14.3%)	1 (14.3%)
Other Physicians	n=4	4 (100%)	-	-	-
Occupation Not Disclosed	n=1	-	-	-	1 (100%)

* Agree = Strongly Agree or Moderately Agree
** Disagree = Strongly Disagree or Moderately Disagree

Table 18: Analysis of Factor " Do not have to create or reset and remember a new password" by Sex, Age and Occupation

Factor: Not having to create / reset and remember a New Password Every 3/6 months for using an email different from the email provided by your organization	Sample Size	Agree*	Neither Agree Nor Disagree	Disagree**	No Answer
All Respondents	n=19	15 (79%)	1 (5.3%)	1 (5.3%)	2 (10.5%)
Sex					
Men	n=15	12 (80%)	1 (6.7%)	1 (6.7%)	1 (6.7%)
Women	n= 3	3 (100%)	-	-	-
Sex Not Disclosed	n= 1	-	-	-	1 (100%)
Age Group					
<30 Years	n=3	3 (100%)	-	-	-
30-39 Years	n=4	2 (50%)	1 (25%)	1 (25%)	-
40-49 Years	n=8	7 (87.5%)	-	-	1(12.5%)
50-59 Years	n=3	1 (100%)	-	-	-
>60 Years	n=1	-	-	-	1 (100%)
Occupation					
Primary Care Physicians	n=7	6 (85.7%)	1 (14.3%)	-	-
Specialists	n=7	5 (71.4%)	-	1 (14.3%)	1 (14.3%)
Other Physicians	n=4	4 (100%)	-	-	-
Occupation Not Disclosed	n=1	-	-	-	1 (100%)

* Agree = Strongly Agree or Moderately Agree
** Disagree = Strongly Disagree or Moderately Disagree

Table 19: Analysis of Factor "Confidence/ sense of security that data transfer complies with regulations" by Sex, Age Group and Occupation

Factor: My confidence/ sense of security that my data transfer complies with regulations related to privacy and security of patient information	Sample Size	Agree*	Neither Agree Nor Disagree	Disagree**	No Answer
All Respondents	n=19	14 (73.7%)	3 (15.8%)	1 (5.3%)	1 (5.3%)
Sex					
Men	n=15	11 (73.3%)	3 (20%)	1 (6.7%)	-
Women	n= 3	3 (100%)	-	-	-
Sex Not Disclosed	n= 1	-	-	-	1 (100%)
Age Group					
<30 Years	n=3	2 (66.7%)	1 (33.3%)	-	-
30-39 Years	n=4	3 (75%)	-	1 (25%)	-
40-49 Years	n=8	6 (75%)	1 (12.5%)	-	1(12.5%)
50-59 Years	n=3	2 (66.7%)	1 (33.3%)	-	-
>60 Years	n=1	1 (100%)	-	-	-
Occupation					
Primary Care Physicians	n=7	7(100%)	-	-	-
Specialists	n=7	4 (57.1%)	2 (28.6%)	1 (14.3%)	-
Other Physicians	n=4	3 (75%)	1 (25%)	-	-
Occupation Not Disclosed	n=1	-	-	-	1 (100%)

* Agree = Strongly Agree or Moderately Agree
** Disagree = Strongly Disagree or Moderately Disagree

Table 20: Analysis of Perceived Usefulness of "ST-SecRx is More Secure" by Sex, Age Group and Occupation

ST-SecRx is more secure compared to previously used methods of patient data exchange through email	Sample Size	Agree*	Neither Agree Nor Disagree	Disagree**	No Answer
All Respondents	n=19	12 (68.4%)	3 (15.8%)	1 (5.3%)	2 (10.5%)
Sex					
Men	n=15	10 (66.7%)	3 (20%)	1 (6.7%)	1 (6.7%)
Women	n= 3	3 (100%)	-	-	-
Sex Not Disclosed	n= 1	-	-	-	1 (100%)
Age Group					
<30 Years	n=3	3 (100%)	-	-	-
30-39 Years	n=4	3 (75%)	-	1 (25%)	-
40-49 Years	n=8	7 (87.5%)	-	-	1 (12.5%)
50-59 Years	n=3	1 (33.3%)	2 (66.7%)	-	-
>60 Years	n=1	-	-	-	1 (100%)
Occupation					
Primary Care Physicians	n=7	6 (85.7%)	1 (14.3%)	-	-
Specialists	n=7	4 (57.1%)	1 (14.3%)	1 (14.29%)	1 (14.3%)
Other Physicians	n=4	3 (75%)	1 (25%)	-	-
Occupation Not Disclosed	n=1	-	-	-	1 (100%)

* Agree = Strongly Agree or Moderately Agree
** Disagree = Strongly Disagree or Moderately Disagree

Table 21: Analysis of Perceived Usefulness of "ST-SecRx is Easy to Use" by Sex, Age Group and Occupation

ST-SecRx is easy to use compared to previously used methods of patient data exchange through email	Sample Size	Agree*	Neither Agree Nor Disagree	Disagree**	No Answer
All Respondents	n=19	10 (52.6%)	5 (26.3%)	1 (5.3%)	3 (15.8%)
Sex					
Men	n=15	9 (60%)	4 (26.7%)	-	2 (13.3%)
Women	n= 3	1 (33.3%)	1 (33.3%)	1 (33.3%)	-
Sex Not Disclosed	n= 1	-	-	-	1 (100%)
Age Group					
<30 Years	n=3	1 (33.3%)	2 (66.7%)	-	-
30-39 Years	n=4	1 (25%)	2 (50%)	-	1 (25%)
40-49 Years	n=8	7 (87.5%)	-	-	1 (12.5%)
50-59 Years	n=3	1 (33.3%)	1 (33.3%)	1 (33.3%)	-
>60 Years	n=1	-	-	-	1 (100%)
Occupation					
Primary Care Physicians	n=7	5 (71.4%)	1 (14.3%)	-	1 (14.3%)
Specialists	n=7	4 (57.1%)	1 (14.3%)	1 (14.3%)	1 (14.3%)
Other Physicians	n=4	1 (25%)	3 (75%)	-	-
Occupation Not Disclosed	n=1	-	-	-	1 (100%)

* Agree = Strongly Agree or Moderately Agree
** Disagree = Strongly Disagree or Moderately Disagree

Table 22: Behavioral Intention to "Take Advantage" of ST-SexRx by Sex, Age Group and Occupation

If ST-SecRx is available to me, I intend to take advantage of it when exchanging patient data	Sample Size	Agree*	Neither Agree Nor Disagree	Disagree**	No Answer
All Respondents	n=19	14 (73.9%)	3 (15.8%)	1 (5.26%)	1 (5.26%)
Sex					
Men	n=15	12 (80%)	2 (13.3%)	1 (6.7%)	-
Women	n= 3	2 (66.7%)	1 (33.3%)	-	-
Sex Not Disclosed	n= 1	-	-	-	1 (100%)
Age Group					
<30 Years	n=3	3 (100%)	-	-	-
30-39 Years	n=4	2 (50%)	1 (25%)	1 (25%)	-
40-49 Years	n=8	6 (75%)	1 (12.5%)	-	1 (12.5%)
50-59 Years	n=3	2 (66.7%)	1 (33.3%)	-	-
>60 Years	n=1	1 (100%)	-	-	-
Occupation					
Primary Care Physicians	n=7	6 (85.7%)	1 (14.3%)	-	1 (14.3%)
Specialists	n=7	5 (71.4%)	1 (14.3%)	1 (14.3%)	-
Other Physicians	n=4	3 (75%)	1 (25%)	-	-
Occupation Not Disclosed	n=1	-	-	-	1 (100%)

* Agree = Strongly Agree or Moderately Agree
** Disagree = Strongly Disagree or Moderately Disagree

Table 23: Behavioral Intention to "Likely To Use" ST-SexRx by Sex, Age Group and Occupation

If ST-SecRx is available to me, I am likely to use it more often than other means of patient data exchange through email	Sample Size	Agree*	Neither Agree Nor Disagree	Disagree**	No Answer
All Respondents	n=19	13 (68.4%)	2 (10.5%)	2 (10.5%)	2 (10.5%)
Sex					
Men	n=15	11 (73.3%)	2 (13.3%)	1 (6.7%)	1 (6.7%)
Women	n= 3	2 (66.7%)	-	1 (33.3%)	-
Sex Not Disclosed	n= 1	-	-	-	1 (100%)
Age Group					
<30 Years	n=3	3 (100%)	-	-	-
30-39 Years	n=4	1 (25%)	1 (25%)	1 (25%)	1 (25%)
40-49 Years	n=8	6 (75%)	1 (12.50%)	-	1 (12.5%)
50-59 Years	n=3	2 (66.7%)	-	1 (33.3%)	-
>60 Years	n=1	1 (100%)	-	-	-
Occupation					
Primary Care Physicians	n=7	5 (71.4%)	1 (14.3%)	-	1 (14.3%)
Specialists	n=7	5 (71.4%)	-	2 (28.6%)	-
Other Physicians	n=4	3 (75%)	1 (25%)	-	-
Occupation Not Disclosed	n=1	-	-	-	1 (100%)

* Agree = Strongly Agree or Moderately Agree
** Disagree = Strongly Disagree or Moderately Disagree

Table 24: Behavioral Intention to Use ST-SexRx as "ONLY Means" by Sex, Age Group and Occupation

If ST-SecRx is available to me, I intend to use this as the ONLY means of exchanging patient data through email	Sample Size	Agree*	Neither Agree Nor Disagree	Disagree**	No Answer
All Respondents	n=19	12 (63.2%)	4 (21.2%)	2 (10.5%)	1 (5.3%)
Sex					
Men	n=15	10 66.7%)	4 (26.7%)	1 (6.7%)	-
Women	n= 3	2 (66.7%)	-	1 (33.3%)	-
Sex Not Disclosed	n= 1	-	-	-	1 (100%)
Age Group					
<30 Years	n=3	2 (66.7%)	1 (33.3%)	-	-
30-39 Years	n=4	3 (75%)	-	1 (25%)	-
40-49 Years	n=8	5 (62.5%)	2 (25%)	-	1 (12.5%)
50-59 Years	n=3	1 (33.3%)	1 (33.3%)	1 (33.3%)	-
>60 Years	n=1	1 (100%)	-	-	-
Occupation					
Primary Care Physicians	n=7	5 (71.4%)	2 (28.6%)	-	-
Specialists	n=7	5 (71.4%)	1 (14.3%)	1 (14.3%)	-
Other Physicians	n=4	2 (50%)	1 (25%)	1 (25%)-	-
Occupation Not Disclosed	n=1	-	-		1 (100%)

* Agree = Strongly Agree or Moderately Agree
** Disagree = Strongly Disagree or Moderately Disagree

Table 25: Behavioral Intention to "Likely Use ONLY" ST-SexRx by Sex, Age Group and Occupation

If ST-SecRx is available to me, I am likely to use ONLY this as means of patient data exchange through email	Sample Size	Agree*	Neither Agree Nor Disagree	Disagree**	No Answer
All Respondents	n=19	14 (73.7%)	2 (10.5%)	2 (10.5%)	1 (5.3%)
Sex					
Men	n=15	12 (80%)	2 (13.3%)	1 (6.7%)	-
Women	n= 3	2 (66.7%)	-	1 (33.3%)	-
Sex Not Disclosed	n= 1	-	-	-	1 (100%)
Age Group					
<30 Years	n=3	2 (66.7%)	1 (33.3%)	-	-
30-39 Years	n=4	3 (75%)	-	1 (25%)	-
40-49 Years	n=8	6 (75%)	1 (12.5%)	-	1 (12.5%)
50-59 Years	n=3	2 (66.7%)	-	1 (33.3%)	-
>60 Years	n=1	1 (100%)	-	-	-
Occupation					
Primary Care Physicians	n=7	6 (85.7%)	1 (14.3%)	-	-
Specialists	n=7	6 (85.7%)	-	1 (14.3%)	-
Other Physicians	n=4	2 (50%)	1 (25%)	1 (25%)	-
Occupation Not Disclosed	n=1	-	-	-	1 (100%)

* Agree = Strongly Agree or Moderately Agree
** Disagree = Strongly Disagree or Moderately Disagree

Table 26: Behavioral Intention to Use ST-SexRx on "Would Enhance Effectiveness of Patient's Healthcare" by Sex, Age Group and Occupation

Use of ST-SecRx would enhance my effectiveness in managing my patients' health care	Sample Size	Agree*	Neither Agree Nor Disagree	Disagree**	No Answer
All Respondents	n=19	12 (63.2%)	5 (26.3%)	1 (5.3%)	1 (5.3%)
Sex					
Men	n=15	10 (66.7%)	4 (26.7%)	1 (6.7%)	-
Women	n= 3	2 (66.7%)	1 (33.3%)	-	-
Sex Not Disclosed	n= 1	-	-	-	1 (100%)
Age Group					
<30 Years	n=3	2 (66.7%)	1 (33.3%)	-	-
30-39 Years	n=4	2 (50%)	1 (25%)	1 (25%)	-
40-49 Years	n=8	6 (75%)	1 (12.5%)	-	1 (12.5%)
50-59 Years	n=3	1 (33.3%)	2 (66.7%)	-	-
>60 Years	n=1	1 (100%)	-	-	-
Occupation					
Primary Care Physicians	n=7	6 (85.7%)	1 (14.3%)	-	-
Specialists	n=7	4 (57.1%)	2 (28.6%)	1 (14.3%)	-
Other Physicians	n=4	2 (25%)	2 (50%)	-	-
Occupation Not Disclosed	n=1	-	-	-	1 (100%)

* Agree = Strongly Agree or Moderately Agree
** Disagree = Strongly Disagree or Moderately Disagree

Table 27: Behavioral Intention to Use ST-SexRx on "Reduce Diagnostic Tests" by Sex, Age Group and Occupation

Use of ST-SecRx would reduce duplication of requests for diagnostic tests between different healthcare providers	Sample Size	Agree*	Neither Agree Nor Disagree	Disagree**	No Answer
All Respondents	n=19	11 (57.9%)	4 (21.1%)	3 (15.8%)	1 (5.3%)
Sex					
Men	n=15	9 (60%)	4 (26.7%)	2 (13.3%)	-
Women	n= 3	2 (66.7%)	-	1 (33.3%)	-
Sex Not Disclosed	n= 1	-	-	-	1 (100%)
Age Group					
<30 Years	n=3	2 (66.7%)	1 (33.3%)	-	-
30-39 Years	n=4	2 (50%	1 (25%)	1 (25%)	-
40-49 Years	n=8	4 (50%)	2 (25%)	1 (12.5%)	1 (12.5%)
50-59 Years	n=3	1 (33.3%)	-	1 (33.3%)	1 (33.3%)
>60 Years	n=1	1 (100%)	-	-	-
Occupation					
Primary Care Physicians	n=7	5 (71.4%)	1 (14.3%)	1 (14.3%)	-
Specialists	n=7	4 (57.1%)	1 (14.3%)	2 (28.6%)	-
Other Physicians	n=4	2 (50%)	2 (50%)	-	-
Occupation Not Disclosed	n=1	-	-	-	1 (100%)

* Agree = Strongly Agree or Moderately Agree
** Disagree = Strongly Disagree or Moderately Disagree