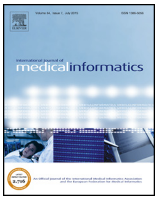
International Journal of Medical Informatics 100 (2017) 63–76

Contents lists available at ScienceDirect

International Journal of Medical Informatics

journal homepage: www.ijmijournal.com



The impact of secure messaging on workflow in primary care: Results of a multiple-case, multiple-method study

Peter L.T. Hoonakker[a,*], Pascale Carayon[a,b], Randi S. Cartmill[c]

[a] Center for Quality and Productivity Improvement (CQPI), University of Wisconsin-Madison, 1550 Engineering Drive, Madison, WI 53706, USA
[b] Department of Industrial and Systems Engineering, University of Wisconsin-Madison, 1415 Engineering Drive, Madison, WI 53706, USA
[c] Department of Surgery, University of Wisconsin-Madison, K6/117 s Clinical Science Center, 600 Highland Ave, Madison, WI 53792, USA

ARTICLE INFO

Article history:
Received 27 July 2016
Received in revised form 4 January 2017
Accepted 7 January 2017

Keywords:
Patient portal
Secure messaging
Workflow
Multiple case study
Mixed methods

ABSTRACT

Introduction: Secure messaging is a relatively new addition to health information technology (IT). Several studies have examined the impact of secure messaging on (clinical) outcomes but very few studies have examined the impact on workflow in primary care clinics. In this study we examined the impact of secure messaging on workflow of clinicians, staff and patients.
Methods: We used a multiple case study design with multiple data collections methods (observation, interviews and survey).
Results: Results show that secure messaging has the potential to improve communication and information flow and the organization of work in primary care clinics, partly due to the possibility of asynchronous communication. However, secure messaging can also have a negative effect on communication and increase workload, especially if patients send messages that are not appropriate for the secure messaging medium (for example, messages that are too long, complex, ambiguous, or inappropriate).

Results show that clinicians are ambivalent about secure messaging. Secure messaging can add to their workload, especially if there is high message volume, and currently they are not compensated for these activities. Staff is –especially compared to clinicians- relatively positive about secure messaging and patients are overall very satisfied with secure messaging.

Finally, clinicians, staff and patients think that secure messaging can have a positive effect on quality of care and patient safety.
Conclusion: Secure messaging is a tool that has the potential to improve communication and information flow. However, the potential of secure messaging to improve workflow is dependent on the way it is implemented and used.

1. Introduction

Secure messaging is electronic communication about relevant health information between a patient and a health care provider that ensures that only those parties can access the communication [1]. The messages are encrypted and integrity-protected in accordance with standards for encryption and hashing algorithms. In the United States, any electronic communication between patient and provider needs to conform to regulations in the Health Insurance Portability and Accountability Act (HIPAA).[1] The first secure messaging systems were implemented more than 10 years ago, mostly

[*] Corresponding author at: Center for Quality and Productivity Improvement (CQPI), University of Wisconsin-Madison, 3124 Engineering Centers Building, 1550 Engineering Drive, Madison, WI 53706, USA.
E-mail address: peter.hoonakker@wisc.edu (P.L.T. Hoonakker).

[1] HIPAA means that electronic communication between patients and providers needs to meet the following requirements: Healthcare messaging and personal messaging are segregated; special authorization and authentication for accessing messages through a personal invitation process is required and access to messages is password-protected; messages are encrypted in transit; data on mobile devices is encrypted; personal Health Information (PHI) is removed from screen notifications; message histories are fully archived; there are auditing capabilities; if photo sharing is allowed, photos taken are not added to devices' camera rolls, and they are encrypted, secured, and auditable; copying or leaking of PHI is made very difficult (e.g. copying on a clipboard is not possible); if devices are stolen it should be possible to instantly lockout and erase data. All of this means that communication between patients and providers using a personal e-mail account for sending a message, or sending a message through an app (e.g. Facebook) is not conform HIPAA regulation.

http://dx.doi.org/10.1016/j.ijmedinf.2017.01.004
1386-5056/© 2017 Elsevier B.V. All rights reserved.

as stand-alone systems. Now secure messaging is often a function of a web-based patient portal.

In an early study on secure messaging, Liederman et al. [2] examined the impact of the technology on patient, provider and staff satisfaction, and provider message volume. The authors concluded that uptake of secure messaging was slow; one year after implementation, 6394 patients out of a patient panel of 135,000 patients (4.7%) were enrolled in secure messaging. These patients sent 6731 messages in 6 months, fewer than 21% sent 4 or more messages; 34% sent 2–3 messages, and nearly half (45%) sent a single message. Several other studies have found low adoption rates for secure messaging [3–5]. Goel et al. [4] examined the reasons for the low uptake of patient portals and secure messaging. Results showed that most respondents (63%) did not attempt enrollment because of lack of information or motivation (did not know about the portal, or did not have instructions; forgot, was too busy). Another 30% did not enroll because of negative attitudes towards the portal (did not think it would be useful, preferred phone over secure messaging).

1.1. Secure messaging and workflow

Relatively few studies have examined the impact of secure messaging on workflow. Workflow is the flow of people, equipment, information and tasks, in different places, at different levels, at different timescales continuously and discontinuously, that are used or required to support the goals of the work domain [6]. From a human factors perspective, workflow includes communication, coordination, searching for and interacting with information, problem-solving and planning. Secure messaging can both support workflow, for example by facilitating communication, and hinder workflow, for example by interrupting work processes. One of the main questions about secure messaging is whether it replaces existing workflows such as telephone contacts or clinic visits or it adds to it, by creating a new "channel of communication" and thereby possibly adding to workload. Until recently, most providers dealing with secure messages were not compensated for these activities, but this is starting to change as we are moving toward a global payment system [7]. Liederman et al. [2] and Zhou et al. [8] examined the impact of secure messaging on primary care utilization. Results showed that access to secure messaging was associated with decreased rates of both office visits and telephone contacts.

Several studies have examined the impact of patient portal on *workload*. The impact of online messaging on workload is not consistent: several studies report an increase in workload [9,10], [11,37]; some studies report a temporary increase in workload that afterwards plateaus [12]; Grover et al., 2005); and other studies report a reduction in workload [13,14]; Wallwiener et al., 2010). In most of these studies workload was measured at the *clinic level* (e.g., volume of secure messages compared to telephone call volume), and not at the individual level. In other words, it is difficult to determine whether providers or staff experienced a change in their workload. Some studies examined the volume of secure messages per provider. Several studies show that volume of secure messages is low (approximately two secure messages per day per provider), and that providers spend about 5–10 min a day responding to them [15,16,2]. A study by Lin et al. [17] found that providers received on average one message per day from 250 patients with access to secure messaging.

Several studies examined the effect of the information that patients provide electronically on *communication*. Many studies focused on the volume of patient-provider communication, but some studies have also examined the quality of communication. In a systematic review, Ye et al. [18] examined the role of secure messaging in patient-provider communication. The benefits of secure messaging were recognized by both patients and providers, and several studies concluded that secure messaging has great potential to improve patient-provider communication [19–21]. Some of the studies in the review analyzed the content of the secure messages exchanged between patient and provider. Most of the secure messages were about non-acute issues, but a study by Rosen and Kwoh [22] found that nearly 6% of secure messages were urgent, and 0.002% required a physician's immediate attention. Several studies examined the characteristics of secure messages and noted that messages were mostly brief, formal and medically relevant [23–25]. The study by Roter et al. [23] compared the content of messages sent by patients with those sent by providers to their patients. Provider messages in general were shorter and more direct than patient messages. Patients were generally satisfied with secure messaging [19,20].

The literature shows that most studies that examine the impact of health IT on workflow focus on large healthcare organizations [26]. Small and medium-sized practices are likely to need the most help in analyzing their workflows as they typically do not have access to IT support and quality improvement resources. Therefore, in this study, we examined the impact of secure messaging on workflow in small and midsized practices. Most of the literature has focused on the impact of secure messaging on the work of clinicians. Very few studies have examined the impact on the work of clinic staff. In this study, we examined the impact of secure messaging on workflow of clinicians, staff and patients.

1.2. Research questions

1 What is the perceived impact of secure messaging on quality of care and patient safety and how satisfied are end-users (clinicians, staff and patients) with secure messaging?
2 What does the secure messaging workflow look like?
3 What are workflow facilitators and barriers to secure messaging for clinicians, staff and patients?

2. Methods

2.1. Study design

This study uses a multiple case study design with mixed methods for data collection [27,28]. The five participating clinics (i.e., five cases) are primary care clinics that happen to be located in medium-sized cities. One clinic is located in the Southeastern United States and four clinics are in the Midwestern United States.

2.2. Setting and sample

Clinic and respondent characteristics are summarized in Table 1.

2.3. Data collection procedures

2.3.1. Pre-visit questionnaire

Prior to the data collection visit, we held a conference call with the clinic manager and/or physician leader to explain the research study and organize logistics for the site visit. We also used a pre-visit questionnaire to collect data on clinic characteristics (e.g., year when clinic was founded) and the implementation of health IT applications (see Table 1).

2.3.2. Combined observations and interviews

During the data collection site visit, often observations were conducted concurrently with interviews of clinicians and staff. We conducted 39 observations/interviews with clinicians; 13 observations/interviews with clinic staff, and 27 interviews with patients. In total, the observations and interviews with clinicians, staff and patients in the 5 clinics lasted nearly 60 h (see Table 2).