Unintended, Negative Consequences of IT Implementations in Healthcare Minitrack

Virginia Ilie, Ph.D. (Primary Contact)
California Lutheran University
vilie@callutheran.edu

Sweta Sneha, Ph.D.
Kennesaw State University
ssneha@kennesaw.edu

Paul Witman, Ph.D.
California Lutheran University
pwitman@callutheran.edu

1. Minitrack Introduction

Research on the positive aspects of Information Technology (IT) implementations in healthcare abounds. Electronic medical record systems (EMR) and other advanced IT solutions have the potential to reduce healthcare costs, increase quality of care, standardize best practices and allow physicians and patients access to interoperable medical records globally.

However, there are many potential negative aspects and consequences associated with complex IT implementations in healthcare that remain under-researched. Such negative consequences can range from misuse of EMR systems, increased physician workload, workflow inefficiencies, dehumanizing of the patient-provider interaction, user workarounds, physician/nurse/patient dissatisfaction to security attacks and hospital data hacking and ransomware, patient privacy issues, increased hospital costs, HIPAA violations, increased difficulties in information sharing among healthcare entities, and abandonment of costly EMR projects among many other things.

This minitrack focuses on research associated with any unintended, negative aspects of IT implementations in the healthcare domain at various levels of analysis, individual, organizational or societal. Such research should help inform both academics and practitioners of unintended negative consequences from complex IT implementations and introduce possible solutions to alleviate such negative impacts.

2. Paper submissions

Six papers were accepted for presentations in this minitrack (one was withdrawn). All papers touched upon unintended consequences related to system implementations in the healthcare field.

Paper 1: *Demigods of Technology Use – How Beating the Overconfidence Bias Can Prevent Medical Errors* is by a group of researchers from the University

of Sweden, Frederike Marie Oschinsky, Marius Müller and Bjoern Niehaves. This paper looks at the impact of human cognitive biases in the physicians' decision-making process and their impacts on medical error occurrences. Cognitive biases, defined as errors in the thinking process based on an attempt to over simplify information processing, may result in the wrong conclusions when interpreting the information. This research in progress paper proposes a mixed-method investigation into how cognitive biases may be related to unintended outcomes including avoidable hospitalizations, complications related to a procedure, unnecessary tests or medication, and overall, medical errors.

Paper 2: *Points of Failure: A Systematic Review of Information-Flow using Medication Use Cases* is by Rebecca Hermon and Patricia Williams from Australia. This paper investigates medical error occurrences in the clinical information flow (diagnosis – treatment – post treatment) in the primary care system in Australia. Results from a case study suggest that a general practitioner working with computerized systems, is more likely to make a mistake during the treatment stage when prescribing a medication to a patient. This type of error has a snowball effect and will result in other errors such as a wrong prescription.

Paper 3: *Measuring Cyber Security Awareness within Groups of Medical Professionals in Poland* is by Tomasz Hyla and Luiza Fabisiak from Poland. Cyberattacks in the healthcare industry can have many negative consequences on the availability, confidentiality and integrity of medical records and can pose serious risks to patients via medical identity thefts. Using a survey based on cybersecurity recommendations from the European Union Agency for Network and Information Security and the U.S. Department of Health and Human Services, the authors study the cybersecurity awareness of medical professionals in Poland. Results paint a rather dark picture with respect to the clinical providers'

knowledge regarding information security in Poland. These results are worry some since cyber attackers could exploit the weakest link – the medical professionals rather than technical security measures.

Paper 4: *Creating a Standardized Risk Assessment Framework Library for Healthcare Information Technology* is by Suzanna Schmeelk from St John's University in the US. This paper proposes a standardized, open source risk management library for the healthcare domain. This standardized library should provide researchers and healthcare organizations with a useful and consistent framework they can use to jump start or enhance their own risk management assessment and implementation. Most importantly, such library should help alleviate potential data breaches in the healthcare field given its focus on risk prevention.

Paper 5: *The Why of Abandonment: Effects of Team Diversity and Leadership Type on the Disbandment and Stagnation of Online Medical Teams* is by Jiaying Li, Hong Wu and Zhaohua Deng from China. This research focuses on online, virtual medical teams and their recent expansion in China. While virtual medical teams can provide remote consultations and bring patients and providers together via online communication platforms, they are also prone to unintended consequences such as dissolution and disbandment. This study investigates the influence of various factors such as team leadership type and diversity on team dissolution and stagnation of virtual medical teams. Using logistic regression (with the dependent variable being status of the virtual team: 1 – team disbanded), the authors tested an empirical model with a sample of 1,071 virtual medical teams. Results suggest that the state of virtual medical team is influenced by the interaction of team diversity and leadership type, thus such interaction could reduce the possibility of team abandonment.