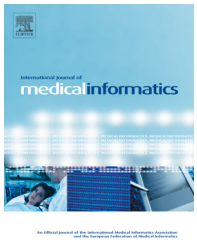
INTERNATIONAL JOURNAL OF MEDICAL INFORMATICS 83 (2014) 140–158

journal homepage: www.ijmijournal.com



The Natural Hospital Environment: A Socio-Technical-Material perspective

Juanita Fernando[a,*], *Linda Dawson*[b,1]

[a] *Faculty Medicine, Nursing & Health Sciences, Monash University, Wellington Road, Monash, VIC 3800, Australia*
[b] *Faculty of Social Sciences, University of Wollongong, NSW 2522, Australia*

ARTICLE INFO

Article history:
Received 24 May 2012
Received in revised form
21 October 2013
Accepted 21 October 2013

Keywords:
Delivery of health care
Medical informatics
Computer security
Health information technology
Framework
Evaluation
Organisational framework
Model
Technology framework
Environment
Outcomes

ABSTRACT

Objectives: This paper introduces two concepts into analyses of information security and hospital-based information systems – a Socio-Technical-Material theoretical framework and the Natural Hospital Environment.

Method: The research is grounded in a review of pertinent literature with previously published Australian (Victoria) case study data to analyse the way clinicians work with privacy and security in their work. The analysis was sorted into thematic categories, providing the basis for the Natural Hospital Environment and Socio-Technical-Material framework theories discussed here.

Results: Natural Hospital Environments feature inadequate yet pervasive computer use, aural privacy shortcomings, shared workspace, meagre budgets, complex regulation that hinders training outcomes and out-dated infrastructure and are highly interruptive.

Discussion: Working collaboratively in many cases, participants found ways to avoid or misuse security tools, such as passwords or screensavers for patient care. Workgroup infrastructure was old, architecturally limited, haphazard in some instances, and was less useful than paper handover sheets to ensure the quality of patient care outcomes.

Despite valiant efforts by some participants, they were unable to control factors influencing the privacy of patient health information in public hospital settings.

Conclusion: Future improvements to hospital-based organisational frameworks for e-health can only be made when there is an improved understanding of the Socio-Technical-Material theoretical framework and Natural Hospital Environment contexts. Aspects within control of clinicians and administrators can be addressed directly although some others are beyond their control. An understanding and acknowledgement of these issues will benefit the management and planning of improved and secure hospital settings.

1. Introduction

In this paper we introduce the concept of a Natural Hospital Environment (NHE) within a Socio-Technical-Material (STM) framework in order to understand and address information security issues in the management of hospital-based e-health information systems. 'E-Health' refers to the application of facsimiles, computers, fixed telephones, mobile telephones and other information and communication devices to support patient care. 'Information security' is difficult to define but tends to incorporate data confidentiality, data integrity

* *Corresponding author*. Tel.: +61 3 990 58537/408 131 535.
E-mail addresses: juanita.fernando@monash.edu (J. Fernando), lindad@uow.edu.au (L. Dawson).
[1] Tel.: +61 2 4221 3821.

1386-5056/$ – see front matter © 2013 Elsevier Ireland Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.ijmedinf.2013.10.008

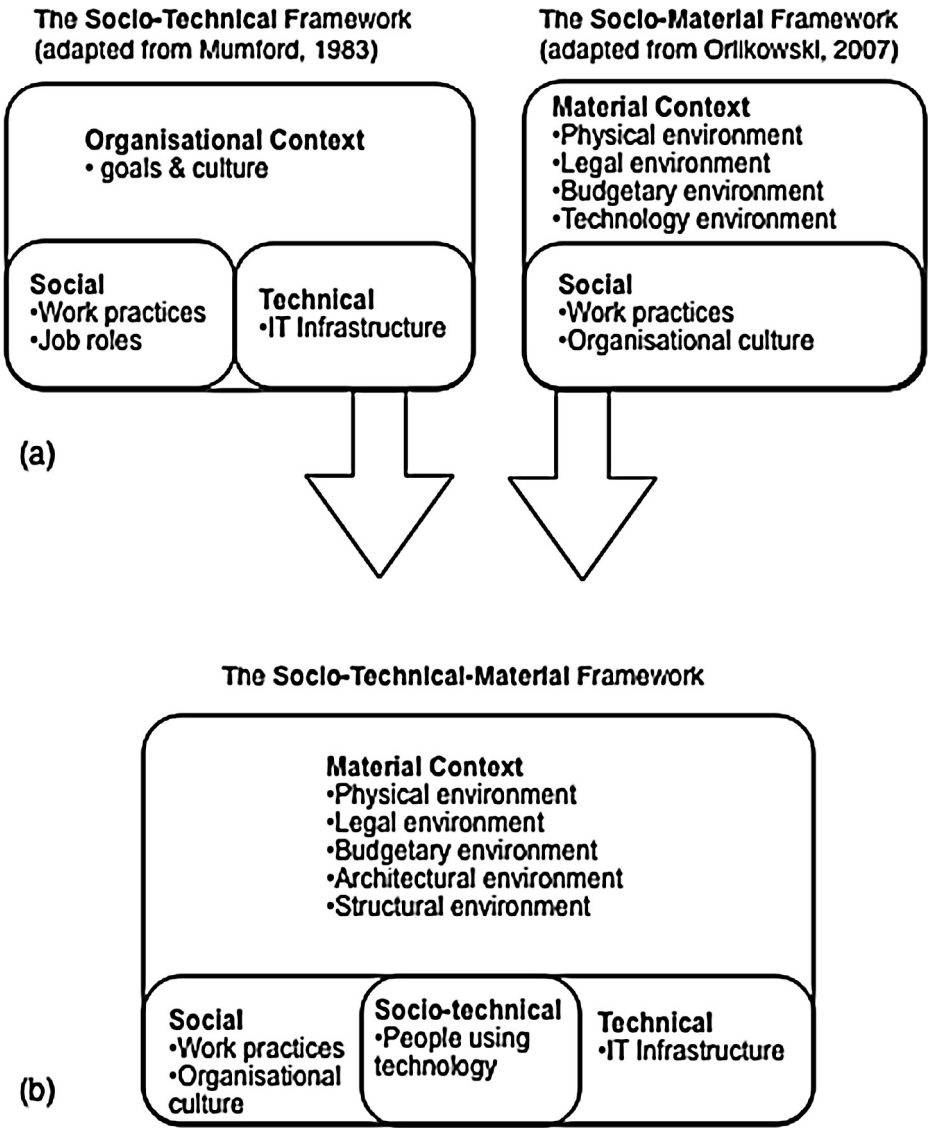


Fig. 1 – The development of the Socio-Technical-Material (STM) framework – encompassing socio-technical and socio-material frameworks.

and data availability. Data is *confidential* when information is accessible only to those with the required level of authorisation. Data *integrity* refers to the accuracy and completeness of information and processing methods. Data *availability* means that all authorised end users can obtain information when and where it is required. We refer to the concepts of confidentiality, integrity and availability as "security" in this manuscript. Data security is a fundamental health privacy principle and central to analysis of privacy and security (P&S) in this context [1].

Evidence also links the introduction of e-health at the clinical user level to a range of security issues hampering the quality of sustained patient care outcomes [2–5]. Clinical user level communities include nurses, doctors and allied health professionals, who need mobile access to data and information in patient care environments [6].

A Socio-Technical-Material framework for the NHE: In order to better understand and define a Natural Hospital Environment (especially in public, government-funded hospitals) we initially consider the NHE to include shared clinical workspaces and shared computer equipment within a physical surrounding and a set of regulatory guidelines that are both hospital-specific and part of government legislation. So the NHE is both a good example of a socio-technical system and a socio-material context. Further, literature analysing e-health implementations [3,6–14] indicate that a combination of the socio-technical and the socio-material into a single framework may offer a useful lens to enhance our understanding of the NHE. We propose a general Socio-Technical-Material framework, Fig. 1(b) which encompasses and adapts elements of socio-technical systems and the socio-material context as defined by Orlikowski (2007), Fig. 1(a) [12].

A socio-technical system is "*. . . one which recognises the interaction of technology and people and produces work systems which are both technically efficient and have social characteristics which lead to high job satisfaction*" [12]. Mumford (1983) further suggests that effective computer systems require technology to fit closely