Chapter 5
The Protocols of Privileged Information Handling in an E-Health Context: Australia

Juanita Fernando
Monash University, Australia

ABSTRACT

In this chapter, the author analyzes adherence to privileged health information handling protocols in the clinical context to inform work plans pioneering an ostensibly private and secure Australian national e-health scheme. The analysis leverages findings from new and emerging literature and data from a study involving twenty-three medical, nursing, and allied health clinicians working at public hospitals in Victoria, combined with data collected for a new case study from nine information technology (IT) support staff working at the same hospitals. In both case studies, data collection was based on the Questerview technique to examine the privacy of clinical e-health work for patient care. The research approach provided a rich source of qualitative data for analysis.

The evidence suggests a socio-material mismatch between privileged information handling protocols and clinical work in the natural hospital environment. The protocols foster a range of information privacy threats that may affect patient care outcomes. The risks incorporate data confidentiality, integrity, and availability. That is, health data is accessible only to those with the required level of authorization, it is accurate and complete, and all authorized end users can obtain information when and where required. Reflecting international findings, some Australian clinicians avoid or work around the protections provided by health privacy legal frameworks. Although fixes for several privacy threats are available, they do not appear to be in common use. Rather than analyze and rectify privacy threats embedded into the socio-material interface of patient care settings before pioneering e-health schemes, authorities propose to amend the Privacy Act and weaken identification rules to advance the national unified record. At the same time, unresolved work tension exists between clinicians and IT support staff. The mismatch trig-

DOI: 10.4018/978-1-60960-573-5.ch005

gered a series of responses that this chapter argues do not benefit either the clinician or the patient, and may hamper the introduction of a unified Australian e-health scheme more generally.

Health authorities need to review the privacy and security of real-life work contexts before pioneering new, privileged information handling protocols as a foundation of a new national e-health scheme.

INTRODUCTION

Reflecting global trends, Australia is increasingly adopting unified, national electronic health (e-health) frameworks to improve standards of patient care while containing service costs. The term "e-health" refers to the electronic management and exchange of patient health information using information and communication technology (ICT). The ICT includes databases, mobile phones, faxes, computerized devices and the Internet. Threats to health information stored on computer networks are complex and jeopardize the privacy of millions of patient-care records rather than, as reported prior to e-health, perhaps hundreds of paper records per incident (Zajac 2010). Evidence suggests privileged e-health information handling protocols are a broad and complex subject area, yet few studies analyze their impact in relation to complicated social and material, or socio-material, interactions in patient care settings (Orlikowski, 2007; Westbrook *et al.*, 2007). This chapter attempts to rectify the shortcoming, adding to knowledge about the protocols of privileged-information handling and informing national e-health framework strategies.

BACKGROUND

Information privacy and security (P&S), information technology (IT) and health care are complex domains that often use similar language in dissimilar ways. Thus we attempt to provide a shared understanding of the key terms used here. Privileged information handling protocols encompass a wide range of complicated issues and activities, from physical security to technical and administrative security. The convergence between physical security and technical or administrative security threats has contributed to an increasing number of serious incidents in recent years (Zajac, 2010). For the purposes of this chapter we define privileged information handling protocols as all measures that protect information privacy and security.

A false dichotomy often exists between privacy and security. Yet individuals cannot have one without the other. The term "security" refers to all implementations that protect information privacy. "Privacy*"* concerns control over access to information about One's self and associated data, including health information, as enshrined in legislative frameworks (Clarke, 2006). Complete information privacy cannot exist without security while there can be security without complete information privacy.

Clinical work can be subdivided into several tasks or streams. The streams incorporate medical tasks and administrative tasks. Some of the administrative tasks of care provision associated with third party requirements, such as health service organizations, insurance companies, professional associations or governments, are beyond the scope of this study. Medical tasks include clinical observations, assessments of health conditions (such as progress notes and diagnoses) and treatment, and services (such as medication, surgery, physical and psychological therapy). Legislation about medical tasks related to emergency health care are