Chapter VI

Addressing Prescription Fraud in the British National Health Service: Technological and Social Considerations

Athanasia Pouloudi
Brunel University, UK

Prescription fraud constitutes an important drain of health service resources, but one that is difficult to detect and therefore to prevent or rectify. It is expected that the use of information technology in the prescribing process could enhance fraud prevention and detection. For example, electronic prescribing or networking between prescribing stakeholders could facilitate audit. However, the implementation of several computerized solutions in the British National Health Service (NHS) has been problematic. Computerized support for prescribing and fraud prevention is likely to face similar challenges unless the implementation of a technical solution is considered with due attention to the organizational and social context. This chapter presents the problem of prescription fraud in Britain and some of the technological alternatives available for dealing with the problem. The main focus of the chapter, however, is to consider such technological ‘solutions’ in their broader context and examine how technology may limit or may be limited by organizational and social factors, such as the interests and political considerations of the various stakeholders of the prescribing process. In this respect, the chapter provides a useful analysis within which other information systems security issues can be considered.

INTRODUCTION

The provision of effective health care faces significant financial challenges at a global level as demand for medical services and expenditure rises continuously. In developed
countries, 10 to 20 per cent of health expenditure is spent on pharmaceuticals (Abel-Smith, 1994). Pharmaceutical fraud can therefore waste significant amounts of health care resources. Instances of prescription fraud are reported in Europe (e.g., Audit Commission, 1994; Bosch, 1998), in the United States (e.g., Department of Health, 1997; Mintz Levin, 1999; National Drug Strategy Network, 1996), in Canada (e.g., Pharmacare, 1999), and in Australia (e.g., Australian National Audit Office, 1997). Not surprisingly, governments and other stakeholders in medical expenditure are concerned with the effective prevention and detection of fraud.

The Oxford English Reference Dictionary defines fraud as “criminal deception; the use of false representations to gain an unjust advantage”. As such it is an important security issue. Importantly, fraud is an information security issue. On the one hand, its practice relies to a great extent on the lack of effective controls on three main dimensions in security (Bakker, 1998): confidentiality, integrity and accuracy of the information provided by and exchanged between interested parties. On the other hand, information technology can be an important facilitator in fraud prevention and detection as it can contribute to more effective and better-controlled flow of information between legitimate, interested parties. Thus, although fraud has not been explicitly studied as a security issue in most information systems research, it is an important issue in the information security management agenda.

Prescription fraud is a particularly interesting information security management issue because it occurs in an information intensive domain, that of drug use and management. In this domain, information systems are increasingly used to manage information on patients, on drugs, on the costs of drugs as well as to monitor and evaluate the effectiveness of drug use policies (Pouloudi and Whitley, 1997). Furthermore, prescription fraud occurs in a complex context of prescription and dispensing with multiple stakeholders and distinctive structures of responsibility (cf. Backhouse and Dhillon, 1996). Indeed, the British National Health Service (NHS) provides a complex context that has been continuously affected by socio-political factors (Salter, 1998), the strong culture of health care providers (e.g., Little, 1999) and a proactive national information strategy (Department of Health, 1998). Prescription fraud presents therefore an important challenge for information security research, not only because of the important financial stakes, but also because it is an area where information technology can play a significant role. This role is, however, restricted and shaped by the complex social context of the prescribing process and the interests of the stakeholders involved.

The aim of this chapter is to study the phenomenon of prescription fraud in the British NHS by explicitly addressing the interrelations of technological and social considerations. We will argue that these become intertwined and need to be considered in tandem for the effective management of prescription fraud. The focus of this chapter on prescription in community (as opposed to hospital) care provides an opportunity to study the phenomenon in depth. The next section provides an introduction to the phenomenon of prescription fraud in the UK with an overview of the problem as it is currently understood and examples of how fraudulent behavior can occur. The following section introduces the role of information systems as security mechanisms for preventing and detecting prescription fraud, leading on to a discussion that considers the technology within its broader social context. The chapter concludes by stressing the importance of the social dimension in technological solutions: technical and social considerations in prescription fraud and in information security management, which should be jointly studied.
Related Content

Preventing Identity Disclosure in Social Networks Using Intersected Node

Protecting Patient Information in Outsourced Telehealth Services: Bolting on Security When it Cannot be Baked in
[www.igi-global.com/chapter/protecting-patient-information-outsourced-telehealth/45803?camid=4v1a](www.igi-global.com/chapter/protecting-patient-information-outsourced-telehealth/45803?camid=4v1a)

An Ontology of Information Security
[www.igi-global.com/article/ontology-information-security/2468?camid=4v1a](www.igi-global.com/article/ontology-information-security/2468?camid=4v1a)

A "One-Pass" Methodology for Sensitive Data Disk Wipes
[www.igi-global.com/chapter/one-pass-methodology-sensitive-data/20650?camid=4v1a](www.igi-global.com/chapter/one-pass-methodology-sensitive-data/20650?camid=4v1a)