Chapter 65
Human and Organizational Factors of Healthcare Data Breaches:
The Swiss Cheese Model of Data Breach Causation And Prevention

Faouzi Kamoun
Zayed University, UAE

Mathew Nicho
University of Dubai, UAE

ABSTRACT

Over the past few years, concerns related to healthcare data privacy have been mounting since healthcare information has become more digitized, distributed and mobile. However, very little is known about the root cause of data breach incidents; making it difficult for healthcare organizations to establish proper security controls and defenses. Through a systematic review and synthesis of data breaches literature, and using databases of earlier reported healthcare data breaches, the authors re-examine and analyze the causal factors behind healthcare data breaches. The authors then use the Swiss Cheese Model (SCM) to shed light on the technical, organizational and human factors of these breaches. The author's research suggests that incorporating the SCM concepts into the healthcare security policies and procedures can assist healthcare providers in assessing the vulnerabilities and risks associated with the maintenance and transmission of protected health information.

INTRODUCTION

Personal health records (PHR) and electronic health records play an important role in managing health information and enhancing the quality of patients' healthcare through enhanced collection, compilation, storage, tracking and dissemination of health records among healthcare providers (Kierkegaard, 2012). The health sector is characterized by a wealth of ever grow-

DOI: 10.4018/978-1-4666-8756-1.ch065

ing information that is dispersed throughout the healthcare organization and its downstream chain of business associates (BA) which includes any person or entity that creates, receives, maintains, or transmits protected health information (PHI) in fulfilling certain functions or activities for the health organization (HHS, 2013a). At the same time, as the healthcare sector is shifting from paper-based to electronic records, electronic data archives are accumulating in healthcare facilities and administrative agencies (O'Keefe & Connolly, 2011). The exchange of electronic protected health information (ePHI) and electronic health records (EHR) further accentuated the need to protect patients' health information, while guaranteeing easy access and a smooth flow of this information among the authorized entities.

Health information is believed to be among the most sensitive and confidential personal data, with the result that confidential data hemorrhage is exposing healthcare providers to unprecedented legal and financial risks (Johnson, 2009).

According to Johnson (2009) data hemorrhages come from many different sources like ambulatory healthcare providers, acute-care hospitals, physician groups, medical laboratories, insurance carriers, back-offices of health maintenance organizations, and outsourced service providers such as billing, collection, and transcription firms. The effects of data breaches on these parties are manifold. The improper disclosure or misuse of health information can cause serious reputational harm such as discrimination, stigmatization, loss of insurance and/or employment (Kulynych & Korn, 2002). The financial costs of data breaches, which include both direct costs, such as "clean-up" costs, and indirect costs, such as loss of revenues from reputational harm, are perhaps the most damaging factors from an organizational perspective. Data breaches can also lead to privacy violations, medical identity fraud, financial identity theft (such as forged taxation, fake health insurance and drug prescription claims) and identity theft (Johnson, 2009). Thus healthcare information security and privacy is a major ethical and legal issue (Appari & Johnson, 2010). In particular, the ethical principle of personal autonomy suggests that individuals have the right to control all matters related to their own body, including their personal health information (Neame, 2012).This right translates into public expectations and legal requirements that healthcare providers shall secure the privacy and confidentiality of patients' health records. We should note however that regulatory compliance and adoption of privacy policies are not strong indicators of adequate patient privacy protection (e.g. Antón et al., 2007, Antón et al., 2010; Bhatti & Grandison, 2010; Grandison & Bhatti, 2010; Massey et al., 2010).

Despite the ethical and legal obligations of healthcare providers to protect the confidentiality of patients' health records, the past few years have witnessed an increase in the number and scope of reported healthcare data breach incidents. This is due to many factors, including (1) the fact that breach reporting became mandatory in September 2009, (2) the ease at which the healthcare sector can be penetrated, and (3) the wealth of sensitive personal information available and accessible to criminals in a patient's health record. For example, a PHR may reveal personal information (such as name, dates of birth, social security number, address, employer and phone numbers), financial and insurance information (such as bank account, credit card numbers, and insurance numbers) and health information (such as diagnosis results, medications, allergies, addiction problems and treatment types).

Despite all forms of legislations, data encryption, and security technologies made available during the past years, one fundamental question remains that is still not fully addressed: "why do data breaches[1] still occur in the healthcare sector?" While a thorough answer is not evident, this research aims to shed light on the possible causes that might contribute to healthcare data breaches.