Chapter 58
Misuse of 'Break-the-Glass' Policies in Hospitals:
Detecting Unauthorized Access to Sensitive Patient Health Data

Benjamin Stark
Neu-Ulm University of Applied Sciences, Neu-Ulm, Germany

Heinrich Lautenbacher
University Hospital Tübingen, Tübingen, Germany

Heiko Gewald
Neu-Ulm University of Applied Sciences, Neu-Ulm, Germany

Ulrich Haase
Klinikum Stuttgart, Stuttgart, Germany

Siegmar Ruff
DSM DatenSchutzManagement Schurer GmbH, Tübingen, Germany

ABSTRACT

This article describes how the information about an individual's personal health is among ones most sensitive and important intangible belongings. When health information is misused, serious non-revertible damage can be caused, e.g. through making intimidating details public or leaking it to employers, insurances etc. Therefore, health information needs to be treated with the highest degree of confidentiality. In practice it proves difficult to achieve this goal. In a hospital setting medical staff across departments often needs to access patient data without directly obvious reasons, which makes it difficult to distinguish legitimate from illegitimate access. This article provides a mechanism to classify transactions at a large university medical center into plausible and questionable data access using a real-life data set of more than 60,000 transactions. The classification mechanism works with minimal data requirements and unsupervised data sets. The results were evaluated through manual cross-checks internally and by a group of external experts. Consequently, the hospital's data protection officer is now able to focus on analyzing questionable transactions instead of checking random samples.

DOI: 10.4018/978-1-7998-8954-0.ch058

INTRODUCTION

Data privacy is an important issue in hospitals around the world (Menon, Jiang, Kim, Vaidya, & Ohno-Machado, 2014; Ponemon Institute, 2015). Safeguarding sensitive patient health data against unauthorized access is of great concern as information misuse can cause serious irreversible damage (Alhaqbani & Fidge, 2010). Although legislative approaches to data privacy differ across international jurisdictions, the importance of protection is widely acknowledged. Germany is regarded to have one of the strictest jurisdictional regimes for protecting health data privacy (Maier, 2004), although the European Union is in a process to strengthen consumer rights in this respect across all member states through its General Data Protection Regulation (EU 2016/679). Access to patient data is only allowed when necessary to treat the patient. Exceptions to this rule are very limited, e.g. if a physician needs to consult a colleague on a case or for documentation and billing purposes. Failure to comply with these laws constitutes a felony and may result in a custodial sentence.

In small organizational units like general practitioner offices for example, complying with these laws is comparatively easy due to fewer users with data access rights and stronger social control amongst peers as compared to larger and more anonymous organizations. For large institutions like a hospital with several thousand data access transactions daily in a 24/7 operational mode protecting data privacy is a major challenge. In order to deal with the high volume of transactions hospitals typically use role-based access policies. However, due to the specific circumstances in hospitals, it is necessary to allow exceptions to the role-based privileges. This is, for example, the case in an emergency, when it is important that "delivery of care comes first" (Ardagna et al., 2010, p. 850). To enable data access which is not compliant with the role-based model but necessary in an emergency, hospital information systems typically adopt an emergency access policy which enables users to bypass their role-based access restrictions. This is referred to as 'Break-the-Glass" (BTG) access, which draws its name from breaking the glass to pull a fire alarm (Ardagna et al., 2010; Brucker & Petritsch, 2009; Zhao & Johnson, 2010). BTG access inevitably raises compliance concerns that patients' data privacy rights may be jeopardized because all employees trained to respond to medical emergencies are able to access confidential data, even if there is no medical reason to do so (Akowuah, Yuan, Xu, & Wang, 2013; Ardagna, De Capitani di Vimercati, Grandison, Jajodia, & Samarati, 2008; Atluri & Pernul, 2014; Y. Chen, Ramamurthy, & Wen, 2013; Eargle et al., 2012). Anecdotal evidence (Gorman & Sewell, 2013; Ornstein, 2008; Porter, 2010) shows that this behavior poses a serious problem and happens more often than generally assumed (Eargle et al., 2012). These abuses of system access rights by employees to gain personal benefits are far more frequent than security breaches from the outside (Y. Chen et al., 2013; Eargle et al., 2012; Li & Shaw, 2008; Medlin, Cazier, & Foulk, 2008; Wen & Tarn, 2001). Especially persons of public interest such as movie stars, famous politicians and other celebrities who are admitted to the hospital are assumed to be frequent victims of BTG misuse (Gorman & Sewell, 2013; Menon et al., 2014; Ornstein, 2008; Porter, 2010). To prevent rogue data access, hospitals need mechanisms beyond organizational guidelines to ensure that patient data is being accessed only when medically necessary (Eargle et al., 2012; Ponemon Institute, 2015). One way to do this is to implement mechanisms that help to detect data access without corresponding medical task.

To support this effort, we conducted a study in cooperation with a large university medical center (UMC) in Germany, analyzing real-life data of more than 60,000 transactions to develop a BTG-misuse detection mechanism. As the medical environment is yet too complex for a fully automated system the goal was to develop an algorithm able to identify those transactions which have a high probability to be