Chapter 7
Auditing Privacy for Cloud-Based EHR Systems

Jonathan Sinclair
RepKnight Ltd., UK

Benoit Hudzia
Stratoscale Ltd., UK

Alan Stewart
Queen's University Belfast, UK

ABSTRACT

An EHR is a modern specialisation of a Customer Relationship Management that specifically focuses on the collection and exchange of electronic health information about individual patients between healthcare organisations. Electronic Heath Records systems hold personally identifiable information, especially that which falls under the category of sensitive personal data. As with all industries, the eHealth industry sees potential in cloud-based service offerings and the reduced infrastructure cost they imply, whilst realising the issues regarding security and privacy that may be encountered from outsourcing processing and storage to untrustworthy Cloud Service Providers (CSPs). In this chapter, the authors propose an approach to handle and audit data privacy requirements by leveraging a carefully designed architecture deployed for auditing data privacy in cloud ecosystems.

INTRODUCTION

Most organisations manage their customer data through a Customer Relationship Management (CRM) system. CRM is a widely adopted strategy for enhancing and maintaining customer relationships and the information that pertains to the customer through the phases of administration, marketing, sales and support. Most commercial CRM offerings didn't provide the support and services required for the health industry and, therefore, a specialised form of CRM, the Electronic Health Record (EHR) system was developed. An EHR is a modern specialisation of a CRM which specifically focuses on the collection and exchange of electronic health information about individual patients between healthcare organisations. EHR systems hold personally identifiable

DOI: 10.4018/978-1-4666-6118-9.ch007

information especially that which falls under the category of sensitive personal data. As with all industries the eHealth industry sees potential in cloud-based service offerings and the reduced infrastructure cost they imply, whilst realising the issues regarding security and privacy that may be encountered from outsourcing processing and storage to untrustworthy CSPs. The loss of control has been highlighted as a concern in regards to the compliance of privacy laws and is required in order to control and enforce the access to records by third parties.

In this chapter, we first propose an approach to defining data privacy requirements. Second, we present an architecture deployed for auditing data privacy. Third we present the validation and verification of a data locality results and finally propose a pragmatic approach to breach of compliance prediction in the light of analysis.

BACKGROUND

E-Health

E-Health refers to the utilisation of information systems within the healthcare industry (I.T. Union 2008). Two goals of e-Health as mentioned by Edworthy (2001) are:

1. To provide greater efficiency; and
2. To scale patient services.

Moreover, the World Health Organisation (WHO) defined e-Health in 2005 as:

Use of information and communications technologies (ICT) in support of health and health-related fields, including health-care services, health surveillance, health literature, health education, knowledge and research.

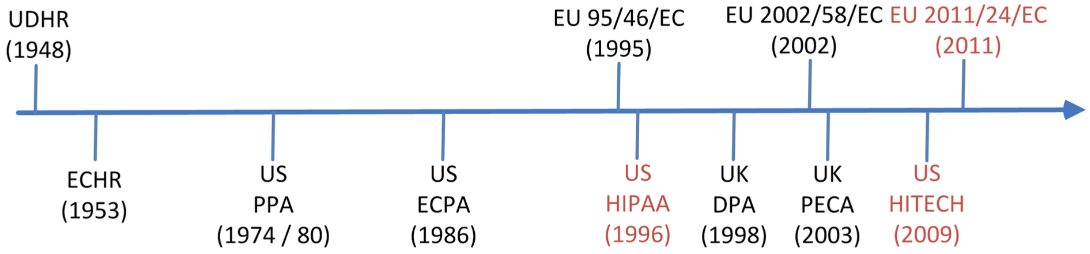
The E-Health domain is heavily regulated, and Figure 1 shows important healthcare laws taken from the EU, UK and US. Current laws highlighted in red; superseded laws are displayed in black. These laws typically address electronic healthcare considerations but do not extend to issues arising from the use of cloud and virtualisation technologies. Revisions of current laws to address issues arising from technological advances are pending.

E-Health Technologies

Various E-Health related technologies have been developed. They aim to provide a unified platform for processing health records, which delivers services to a variety of types of user. But also, enable access to health records from a range of platforms and devices while providing integration of health records across different health-care domains and deliver an efficient health management and administration process.

The recent development and evolution of e-Health systems needs address the economies of

Figure 1. Timeline for healthcare privacy laws


UDHR
(1948)
ECHR
(1953)
US
PPA
(1974 / 80)
US
ECPA
(1986)
EU 95/46/EC
(1995)
US
HIPAA
(1996)
UK
DPA
(1998)
EU 2002/58/EC
(2002)
UK
PECA
(2003)
US
HITECH
(2009)
EU 2011/24/EC
(2011)