Chapter 8
Principles of Information Accountability: An eHealth Perspective

Randike Gajanayake
Queensland University of Technology, Australia

Tony Sahama
Queensland University of Technology, Australia

Renato Iannella
Semantic Identity, Australia

ABSTRACT

Information accountability is seen as a mode of usage control on the Web. Due to its many dimensions, information accountability has been expressed in various ways by computer scientists to address security and privacy in recent times. Information accountability is focused on how users participate in a system and the underlying policies that govern the participation. Healthcare is a domain in which the principles of information accountability can be utilised well. Modern health information systems are Internet based and the discipline is called eHealth. In this paper, the authors identify and discuss the goals of accountability systems and present the principles of information accountability. They characterise those principles in eHealth and discuss them contextually. They identify the current impediments to eHealth in terms of information privacy issues of eHealth consumers together with information usage requirements of healthcare providers and show how information accountability can be used in a healthcare context to address these needs. The challenges of implementing information accountability in eHealth are also discussed in terms of our efforts thus far.

INTRODUCTION

Information accountability (IA) is a solution for usage control on the decentralised Web (Feigenbaum, Hendler, Jaggard, Weitzner, & Wright, 2011; Weitzner et al., 2008). IA is about holding the information users answerable for their actions and the ramifications of those actions. Weitzner et al. (2008) propose a transparent and accountable audit process that gives the users incentives to
abide by the policies put in place and the ability to
determine whether a particular use of information
is policy compliant. Though the concept is not new,
IA is comparatively new to computer science and
information and communication technology (ICT)
and has been interpreted in various dimensions
by computer scientists. These approaches have
been carefully systematised by Feigenbaum et al.
(2012) who state that the term “accountability” is
far broader than just anonymity, identification or
exposure and that it allows actions to be tied to con-
sequences and violations to be tied to punishment.
The approaches considered by Feigenbaum et al.
(2012) define IA in a general context. However,
being a multidimensional concept, IA needs to
be contextualised for its applicability to be better
understood. The lack of contextual definitions
of its underlying principles makes it difficult to
apply in complex domains. Information systems
that utilise the principles of IA are called account-
ability systems. Current technological advance-
ments eliminate the technical barriers previously
present in implementing this type of systems, but
the success of any accountability system depends
on how the underlying policies are formulated,
which in turn depends on the context in which
the systems are implemented.

IA can address several issues in a vast array
of disciplines. Usage control is one area of inter-
est to computer scientists, through which, the
information privacy conundrum can be addressed.
Information privacy has been and still is a major
obstacle to adoption and trust of information sys-
tems; for example in healthcare. Several factors
can be considered when dealing with information
privacy: the type of policies; the nature of partici-
pants and their requirements; data ownership; data
provenance; and the nature of the information such
as sensitivity and availability. These aspects differ
significantly with context. In terms of information
management through electronic media such as
the Internet, privacy can be defined as the degree
of control given to the subject of the informa-
tion (Westin, 1967). Within a given context, the

policies differ in terms of user requirements and
other external factors such as government regula-
tions and organisational policies. The nature of
the information is also a significant reason why
information privacy becomes a critical factor for
information systems. This is clearly evident in
domains such as healthcare (Rindfleisch, 1997).

In this paper, we introduce IA to eHealth as a
means of addressing information privacy. To this
end, we formulate a series of principles for IA
drawn from prior research in computer science.
We contextualise them to eHealth and lay founda-
tions for IA to be utilised in eHealth as a means
of adequate information privacy management.

In what follows, first we identify the problem
addressed in the article and give an introduction
of information accountability. Then, accountable
systems are discussed in terms of their goals and
objectives. The principles of IA are discussed fol-
lowed by a discussion of IA in healthcare including
the need for its implementation in eHealth. Next,
the principles of IA in eHealth are discussed with
the use of the case scenario. Finally, our efforts in
the domain are discussed under a section entitled
implementation challenges and the article is con-
cluded with some closing remarks.

**PROBLEM STATEMENT**

Information privacy concerns are usually coupled
with information security, which mainly involves
unauthorised access to information by external
entities. But, addressing data breaches by author-
rised users pose the biggest challenge and it is
a significant aspect for eHealth systems. Some
even claim that privacy threats are internal factors
and not external (Kierkegaard, 2011). Therefore,
patients have an expectation of confidentiality
in their dealings with any qualified clinician or
healthcare professional (Croll, 2011).

In eHealth, the definition of privacy encompasses
confidentiality, integrity, availability and
accountability (Ishikawa, 2000). The protection