Chapter 14
Ensuring Data Privacy of Employees in Healthcare and Well-Being in the Era of Cloud Computing and the Internet of Things (IoT)

Shashwata Sahu
https://orcid.org/0009-0003-6843-9554
School of Law, KIIT University, Bhubaneswar, India

Navonita Mallick
https://orcid.org/0000-0003-3621-3764
KIIT University, Bhubaneswar, India

Bhupinder Singh
https://orcid.org/0009-0006-4779-2553
Sharda University, India

Kittisak Wongmahesak
https://orcid.org/0009-0000-2129-4691
North Bangkok University, Thailand

Saurabh Chandra
https://orcid.org/0000-0003-4172-9968
Bennett University, India

DOI: 10.4018/979-8-3373-2210-0.ch014

ABSTRACT

Cloud Computing and the Internet of Things have transformed the healthcare landscape in the digital age by improving quality of care and increasing operational efficiency. However, these technologies also entail significant employee data privacy and security risks. The current paper critically explores how the existing legislative measures successfully secure employees' data in the context of such technologies. In particular, a doctrinal research method was adopted to investigate the state of the law in the field and to identify the gaps and weaknesses. The results indicate that the existing rules, namely, the European Union General Data Protection Regulation and Digital Economy Act 2017 are insufficient to protect employee data ownership and access and ensure informed employee consent. In response, the current paper suggests reforming the laws to maintain their effectiveness in the face of rapidly developing technologies.

I. INTRODUCTION

> *"The advancement of technology is based on making it fit in so that you don't even notice it, so it's part of everyday life."*
> *- Bill Gates*

The advancement of Cloud Computing and the Internet of Things in healthcare have fundamentally transformed the industry, enabling significant improvements in employee care, data processing, and operational effectiveness. These technologies allow healthcare data to be stored and accessed in a remote server and transmitted across platforms, making it instantaneous and accessible to healthcare providers at all times (Rejeb et al., 2023). Cloud Computing and the Internet of Things (IoT), support thousands of applications and updates across platforms, which can be effectively used to predict which diseases may be emerging at any given time. The ability of healthcare organisations to utilise such technologies allows for the ability to remotely monitor employees and provide them with real-time predictions of the treatment modalities required for this (Kelly et al., 2020). However, it is essential to note that such advancements also come with significant challenges, with threats to the security of employee data being among the most prominent ones.

The number of cyberattacks against the healthcare sector has increased 350% since 2017. The increase is attributed to the digitisation of medical records and the presence of connected devices, which broaden the attack surface for cyber threats (Samantha Liss & Jasmine Ye Han, 2023). However, the pace at which healthcare integrated IoT and Cloud Computing adversely affected the safety of employee data. With the increased amount of information stored digitally and transmitted at any given