Chapter 5
Designing Trust
From the Core:
Data–Centric Compliance

Hema Lakkaraju

https://orcid.org/0000-0001-5968-8813
Hayag Corp., USA

ABSTRACT

Personalized medicine is the art of customizing healthcare by leveraging and implementing strategic integration of technology and science. Personalized medicine is built on trust between payers, providers, and patients. This digital identity is the core foundation of personalized healthcare. Privacy and security of digital identity in personalized medicine is a combination of mindful patient information flow and inclusion of ethics, strategy, and technology. This chapter describes how to implement a safe and secure digital identity using the concept of designing data-centric compliance or "trust by design."

INTRODUCTION

The fifth industrial revolution brings personalization to the forefront in the healthcare industry. This revolution is a combination of purposeful innovation, inclusivity of technology and human intelligence. This has impacted healthcare to a great extent. This rise of the fifth industrial revolution has led to the rise of a unique and mindful medicine field called personalized medicine. As the healthcare industry is adopting and entering the fifth industrial revolution, it is impossible to say how this revolution will influence the evolution of personalized medicine.

It is an era where personalization is at the forefront in all industries. Personalized medicine is in high demand and will improve the quality of healthy living. It considers the uniqueness of a patient, their genetics, their physiology, and any preexisting conditions, and creates a customized medicine for that individual to cure and prevent rare diseases. In other words, it is one of the core foundations for the future smart healthcare ecosystem.

The heavy transformation of healthcare is digitization of the patient profile, health records, and all possible health-related information. In other words, a digital identity is already being created for each patient in healthcare.

As a result, personalized medicine is rising, and adaptability is slowly increasing. Personalized medicine and healthcare are on high demand and will improve the quality of healthy living. This rise of this emerging field will create a complete patient profile to create customized healthcare. This very existence of the patient's digital identity and building or improving it is the core validation of the patients' existence and their health journey through time.

This all looks promising, but it has its unique challenges. Some challenges include governance and compliance of digital identity and access management. For personalized medicine to happen and effectively work, we need large sets of data. This Big Data needs to be driven from multiple health systems, medical devices, and other healthcare platforms. But this also raises the big concerns- clarity, security, and privacy.

Health data is the core foundation for personalized medicine. Digital data governance needs to be established. Digital and data governance is a critical need and a mandatory framework which can help personalized medicine. This governance includes but not limited to the following

- Understanding which data is important and needed.
- Understanding what data types, sources of critical data.
- Securing the data flow through multiple systems like mobile health apps, AI, wearables, diagnostics, pharma equipment.
- Implementing data intelligence.
- Implementing ethical intelligence.

BACKGROUND

Personalized medicine is based on trust: the trust patients have in payers and providers. Building trust and continuing the bond of trust with patients, improving effective healthcare, and providing unique customized healthcare needs to be done with the privacy and security of patient information in mind.

Related Content

Metamorphic malware detection using opcode frequency rate and decision tree

Mahmood Fazlali, Peyman Khodamoradi, Farhad Mardukhi, Masoud Nosratiand Mohammad Mahdi Dehshibi (2016). *International Journal of Information Security and Privacy (pp. 67-86).*

www.irma-international.org/article/metamorphic-malware-detection-using-opcode-frequency-rate-and-decision-tree/160775

Assessing the Determinants of Adoption of M-Banking by Students: A Study Using an Extended TAM Model

Gazal Punyaniand Sourabh Sharma (2017). *Business Analytics and Cyber Security Management in Organizations (pp. 120-136).*

www.irma-international.org/chapter/assessing-the-determinants-of-adoption-of-m-banking-by-students/171841

Employing Cost Effective Internet-Based Networking Technologies to Manage B2B Relationship: The Strategic Impact on IT Security Risk

Tridib Bandyopadhyay (2012). *International Journal of Risk and Contingency Management (pp. 12-28).*

www.irma-international.org/article/employing-cost-effective-internet-based/65729

Privacy and Security in the Age of Electronic Customer Relationship Management

Nicholas C. Romanoand Jerry Fjermestad (2009). *Techniques and Applications for Advanced Information Privacy and Security: Emerging Organizational, Ethical, and Human Issues (pp. 189-210).*

www.irma-international.org/chapter/privacy-security-age-electronic-customer/30106

Subjective Attack Trees: Security Risk Modeling Under Second-Order Uncertainty

Nasser Al-Hadhrami (2023). *International Journal of Blockchain Applications and Secure Computing (pp. 1-27).*

www.irma-international.org/article/subjective-attack-trees/320498