# The implication of the digitalization of the healthcare on Data Protection and Security

By Herman Ramos

The world is becoming more dependent on digital technologies. These technologies have been revolutionizing some sectors. These proliferations of digital solutions are increasing in the health sector, creating opportunities for old and new challenges in the health sector. With the increase of digital solutions in the health sector, the interaction between patients and doctors have also been moving from face to face in the digital world.

This digital interaction (migration) allows the patient to receive information about medication, about exam results, about future consultation, etc. As a result, there is an increase in access to healthcare outside care settings. In addition, the change to the virtual world means that information of the patient must be collected and stored by the health care.

The increase of cyber tacks, the increase of data breaches, the misuse of data, the lack of cybersecurity strategy and regulation, the non-existence of data protection regulations in some countries has highlighted the need to ensure the protection and security of the Medical data or patient Health Record Data.

In some cases, the lack of data protection and security regulation is affecting the digitalization of healthcare, because there is no guarantee of the protection of the digital integrity of the data. This delay has consequences in the digital transformation of the health industry. This is affecting the digital economy and sustainable development goals especially in obstructing the achievement of Universal health coverage, end of poverty and reduce inequalities.

In this way, is important not only provide the technological solutions to the healthcare industry but guaranty two (2) important aspect:

- Ensure the protection of the Medical Data by implementing the regulatory framework inside the organizations, to implement national and regional laws, and guarantee the accountability, compliance inside the organization. This will certify that the Medical data is being collected, secured and shared in a standardised manner.

- Ensure that the technological solutions used are protected and secure by design. Also must apply different kinds of protection programs and implement cybersecurity strategies inside the organization including the increase of security awareness.

## References

1. Dehling T, Gao F, Schneider S and Sunyaev A. (2015). Exploring the Far Side of Mobile Health: Information Security and Privacy of Mobile Health Apps on iOS and Android. JMIR mHealth and uHealth.
2. Healthcare is a Growing Target for Cybercrime, and It’s Only Going to Get Worse. United States Cybersecurity Magazine 2014; 1: 56.
3. Policy Department for Economic, Scientific and Quality of Life Policies. (2018). Digitalisation and Big Data: Implications for the health sector.
4. Snell E. (2015). Hacking Still Leading Cause of 2015 Health Data Breaches.