

Critical Infrastructure: The future impact of Industry 4.0 on the Security of Healthcare

Newsome, Ashley & Enkhtaivan, Ayush (CYB)

As technology advances and becomes more integrated into healthcare, more data is collected. How that data is stored and used may vary across institutions and countries and there are standards in place to maintain the security of the mass amounts of collected data. In 2003, the Federal Government established the Healthcare and Public Health (HPH) Sector as one of the critical infrastructure sectors in the United States. By doing so, it declares that its security is to the utmost importance to national security, economy, public health, and safety ([dhs.gov](https://www.dhs.gov)).

Critical Infrastructure describes the body of networks and the physical and cyber systems that are vital to the United States' economy security, physical security, and public health and safety such as power grids, water and sewage systems, transportation, banking, emergency systems, and more. There are about 16 different sectors that has been defined by the Department of Homeland Security. One of those sectors is the Health and Public Sector ([dhs.gov](https://www.dhs.gov)), which can be used in threats against national security such as bioterrorism and bioengineering.

Recently critical infrastructure has been moving from Industry 3.0 to Industry 4.0. Industry 4.0 brings together previously separated systems such as information technology (IT) and operational technology (OT) through the interconnection of the technology that makes up Industry 4.0 like IoT/IIoT (Internet of Things/Industrial Internet of Things), big data, cloud computing, and more (Autonomous Manufacturing Ltd.). Most products and processes are transitioning into digital manufacturing by using highly enhanced technologies and methods for better quality and productivity. The industry 4.0 has started to transition the healthcare industry into a smart healthcare industry. For example, the use of IoT BJC HealthCare, a healthcare service provider, has increased and improved operations and efficiency, while reducing cost and providing meaningful real-time visibility across their supply chain.

With the advancements and integration of technology in critical infrastructure, the digitalization of healthcare, the need for physical and cyber security, and the increase in collecting and analyzing big data, the development and move to industry 4.0 has also increased. Industry 4.0, which ties together security (cyber and physical), big data, cyber-physical systems, robotics, integration, IoT (Internet of things), IIoT (Industrial Internet of Things), cloud computing, and more.

In the context of healthcare, industry 4.0 represents various aspects such as telehealth, robotics, IoT and wearable medical devices, mobile health (mHealth) systems and applications. This study explores healthcare as an important aspect of critical infrastructure and how the transition of critical infrastructure to Industry 4.0 will affect the future of healthcare security. This research will be a literature review exploring the growing of Industry 4.0 trend and the digitalization of the healthcare industry and how Industry 4.0 will affect healthcare and the security of healthcare. The literature review will use journal databases such as ScienceDirect and IEEE, in addition to public government documentation on healthcare as a critical infrastructure.