## Report Information

More information from: https://www.marketresearchfuture.com/reports/healthcare-iot-security-market-946

# Healthcare IoT Security Market Research Report - Forecast till 2030

**Report / Search Code:** MRFR/HCIT/0440-CR **Publish Date:** August, 2019

Request Sample

| | | |
|---|---|---|
| **Price** | 1-user PDF : $ 4950.0 | Enterprise PDF : $ 7250.0 |

**Description:**

**Healthcare IoT security Market Overview:** Healthcare IoT Security Market is expected to reach USD 1.12 billion by 2030 at 18.80% CAGR during the forecast period 2022-2030. In traditional times patients used to book appointments with doctors for their check-ups and routine calls or used to use the medium of phones to connect with doctors limiting the point of contact and communication. But, with the introduction of the internet of things, patients and doctors were connected using the internet in the healthcare department. Now doctors can monitor their patients remotely using cameras, microphones, teleprompters, etc. Artificial intelligence with machine learning developed programs ad algorithms for healthcare departments for countries to track and record patient-doctor data which can be used globally concerning patient's consent. With increased global access to Iot in healthcare (Internet of Things), security solutions were introduced to maintain the security and decorum of the medical industry.

With modernization, technology has boosted to a greater level which has led the hospitals to come to homes for tracking and maintaining patients. The introduction of insulin pumps, pacemakers, heartbeat monitors, nasal pumps, and other devices like smartphones and watches to monitor human health has made for the healthcare IoT security market. Government and private organizations play a vital role in maintaining the security of all the home hand-held devices and healthcare institutions.

**COVID-19 Analysis:**

In the November of 2019, the world woke up to an outbreak of a worldwide pandemic that affected countries economically and politically. With the immense loss of man-power countries, economical wealth came to a stand-still. Many countries like Russia, Italy, Brazil, etc. population was diminished to a considerable amount and other countries like the US, India, UK, etc. are facing a rise in active COVID-19 cases on daily basis. Global lockdowns were imposed countrywide and further state-wise to contain the spread of the virus. The Healthcare industry in coordination with the government has played a vital role in tracking and recording the patients and treating them. Healthcare IoT Security Market has shown a boost due to an increased state of emergency to isolate the patients depending on their symptoms and treating them accordingly. Sharing patient's data is at risk and can hamper patient's credibility thus highly secure systems were imposed to share the information across the network.

**Healthcare IoT security Market Dynamics:**

**Drivers:**

Healthcare IoT Security Market is on the verge of growing globally due to the increased demand for real-time data processing of patient records. More customers are inclined in booking doctor's appointments online using hospital services that maintain a schedule between doctor and customer. This helps in the time saving of both customers and doctors by helping in removing the waiting queue. The government of all the 213 countries in the world is concerned with patient-doctor confidentiality thus has imposed HIPPA training for hospital employees to adhere to security. Nowadays our smartphones and watches are acting as health tracking data like a heartbeat monitor, blood pressure, insulin levels, oxygen levels, glucose levels, etc. which needs to be secured to avoid cybercrimes.

**Challenges:**

The major threats that involve the healthcare IoT security industry are easy passwords, poor authentication, loss of data while transfer due to poor network, and other cybercrimes. With an increase in the world's population, there is an increase in patient inventory thus storing the data on-premise has become tougher with time. Thus, cloud-based storage came into the picture. On one hand, this led to easy data access and communication between doctors and patients, but on the other hand, cyber hacking and attacks on internet-connected devices became more vulnerable due to non-secure networks and failed fireball protections.

**Technology Analysis:**

Conventional storage systems are no prompted in healthcare systems due to the introduction of artificial intelligence (to predict the early onset of diseases by analyzing the patient's recording using deep learning). Thus, IoT (Internet of Things) was introduced in the healthcare department where patient's illness history, bill payments, mode of payment, name, age, date of visit, etc. were recorded and stored in hospitals inventory. This in turn is shared across platforms using network hubs making a well connected healthcare system. To maintain cybersecurity government has imposed rules and regulations that each healthcare institution must follow while implementing IoT in the regions to maintain customer satisfaction and security.

**Segment Overview:**

**By Type:**

Healthcare IoT Security Market is segmented as identity management, data loss prevention, access management, data encryption, threat management, system virus management, and data analysis. When a hospital or healthcare center implements IoT Security measures it must follow protocols to maintain security against threats and cybercrimes. A secured ERP system is made for entering the customer's data with is stored in XML files secured by passwords. Virus protection software is installed to fight against unnecessary threats of computer and internet viruses while uploading and downloading documents. Firewalls are initiated to provide prevention against hacking of hardware devices associated with patient monitoring.

**By Vertical:**

Healthcare IoT Security Market is segmented majorly into three categories based on vertical namely: biotechnology (used to maintain the security of user data), Pharma security (used to maintain the security of pharma department against unnecessary threats towards the drug testing or discovery of new drugs or sabotaging the contents of already authorized drugs) and medical device security ( used to avoid the hacking of hardware devices associated with patient monitoring).

**Regional Analysis:**

Healthcare IoT security market trends show development in the private and public healthcare sector where authorities are more concerned with maintaining the industrial standards with agreeing to government regulations. North America is the top-most player when it comes to Healthcare IoT security by securing a global market share of more than 40% in regional accounting and adapting healthcare services to IoT security and privacy. Europe (Russia, Germany, etc.) has contributed about 20% to the global healthcare security market by adhering to global security standards. Asia-Pacific (China, Japan, India, Singapore) have contributed about 40% to new clinical trials of chronic diseases as read by WHO contributing to the rapid increase of the healthcare IoT security industry. Independently Asia-Pacific regions have contributed a CAGR of 47% to the healthcare industry rising the market quotient and revenue by about 2.8 million dollars in the past decade.

**Competitive Landscape:**

The Healthcare IoT security industry has shown tremendous growth since the late 2000s due to increased internet usage throughout the world making it a daily need. The Healthcare IoT security Market has seen a greater number of rural and urban healthcare centers invest in IoT security trends. Many companies have invested in security and firewall-providing industries giving rise to competition between them to prove their worth. Microsoft (US), IBM, Oracle, Intel, Cisco Systems, Deutsche Telekom AG, Agile Cyber Security, Checkpoint Software Technology, Fortinet Inc, Inside Secure SA, Eurotech, Kaspersky, etc., are few of the market key players of healthcare IoT security systems. With more digitalization and artificial intelligence to draw a productive analysis of patient's and doctor's data and chronic diseases, it has become essential to secure healthcare data against any sort of cyber and physical crime that hampers customer's credibility.

**Recent Developments:**

Cisco Systems is one of the best securities providing companies in terms of secured VPNs and two-factor authentication that ensures secure login. Many companies like Oracle, IBM, etc. have been using CISCO security to authenticate the server access to various healthcare industry's data like Pfizer, Ranbaxy. Recently it also acquired a stake of about 1.3 Billion US dollars in Jasper technology to provide a secure connection to maintain healthcare data. Kaspersky and WISekey have been working in collaboration since 2016 to maintain end-to-end security between network hubs for secure and authenticated data transfer. Oracle has used strict firewalls to connect with outside servers to maintain healthcare data entries of companies.

**Report Overview:**

Healthcare IoT Security Market involves end-to-end data security on the cloud-based storage involving the application and network security. Most of the pharmaceutical industries and medical centers have adapted to Healthcare IoT Security companies to maintain the decorum of customer's data. With an increased demand for security for patient's data and real-time data, America, Europe, China, India, Japan, Australia have invested in Healthcare IoT Security Market trends leading to more use of AI and deep learning to process and store this information for maintaining security.

**Table of Content:**