VOL.14 NO.11 PAGES 60 www.expresshealthcare.in

EXPRESS HEALTHCARE

INDIA'S FOREMOST HEALTHCARE MAGAZINE DECEMBER 2021, ₹50

Strategy

Our fight against COVID-19 is far from over:
Dr Sanjay Sarin
Head, FIND India

Healthcare IT
India's digital health mission is the need of the hour but privacy concerns can't be ignored!

AATMANIRBHARTA IN MEDICAL DEVICES CHALLENGES & OPPORTUNITIES

India is at the cusp of a medtech revolution and is poised to be a net exporter like in vaccines and generic drugs

HEALTHCARE IT

Securing medtech through cyber education

Roy Zur, CEO, ThriveDX SaaS highlights the role of cyber education in securing medtech sector

When a healthcare system is attacked, it is not merely on the computers of the hospital but on the patients and the people who take care of them, hence it is more disastrous and threatening.

On October 30th 2021, the healthcare systems at Newfoundland province of Canada were behaving abnormally. They were unable to process the medical appointments and the schedules of the surgery. There was chaos all around in the hospitals and the healthcare system practically came to a halt. An investigation found that a cyber attack on the healthcare systems led to its collapse. Some say that the cyber attack on the healthcare systems could be the worst in the country's history, but it also has repercussions on national security.

Medicine and technology are two different fields, different worlds, but are converging to meet the needs of people in this fast-digitalising world. While this brings convenience and ease, the thieves on the internet are up to creating the nuisance

Is this fear true? indeed it is...

Medicine and technology are two different fields, different worlds, but are converging to meet the needs of people in this fast-digitalising world. While this brings convenience and ease, the thieves on the internet are up to creating the nuisance.

According to a document by World Economic Forum, between June 2020 to October 2021,

"Over 10 million records have been stolen, of every type, including social security numbers, patient medical records, financial data, HIV test results and private details of medical donors. On average, 155,000 records are breached during an attack on the sector, and the number can be far higher, with some incidents reporting the breach of over 3 million records."
https://www.weforum.org/agenda/2021/11/healthcare-cybersecurity/

But, when a healthcare system is attacked, it is not merely on the computers of the hospital but on the patients and the people who take care of them, hence it is more disastrous and threatening.

Digital and connected devices in hospitals

Just as in any other industry, hospitals too have become hi-tech with advanced devices and robotics that can communicate over the internet. With lab machines and reports to doctor's appointments, prescriptions and delivery of medicines at home, digitalisation has covered the entire gamut of healthcare services. Machines like CT scans, MRIs, X-rays are all digital and are interconnected with the hospital management system for smooth flow of patient information.

While it provides quicker services, they are prone to cyberattacks and the motive behind cyberattacks on healthcare companies is clear- it is to fetch very valuable identity and health data of the patient from databases of healthcare service providers like hospitals, clinics, pharmacies, health insurance companies, and other healthcare providers.

Healthcare during pandemic

Pandemic forced adoption of technology in all industries including healthcare. Tele-medicine gained prominence with online consultation, prescription, ordering medicines and payments on the patient portal. But this also made the patient portal an easy target for cyber attackers.

According to a report by Check Point Research, there was a 45% rise in cyber crimes in the healthcare sector around the world and 37% in India, with a total of 2915 incidents in a month during the pandemic which made it one of the most targeted sectors. According to Global Risks Report, 2021, cybersecurity failure is ranked 4th as a part of present danger among the top risks in the next 10 years.

Vulnerability of healthcare system

Experts believe that hackers find telemedicine as an easy target because there is a transfer of data between networks and personal devices and the integration of new technologies with existing ones without having a unified security strategy.

Further, healthcare institutions invest less in security systems. As per statistics, hospitals in India allocate not more than 5% of their budget for cyber security, keeping them vulnerable to cyberattacks.

What can be done?

To mitigate the risks of cyber threats, a multi-pronged strategy needs to be put in place. Efforts are needed from all stakeholders of the industry.

At the policy level, the government should push the Personal Data Protection Act to provide specifics regarding personal data storage and usage. This should apply to medical devices too. At present, all medical devices in India are regulated as "drugs" as per the 'Medical Device Amendment Rules 2020'. While these rules require the devices to be registered with the Drugs Controller General of India, they do not speak about patient data security or privacy within the devices.

At the manufacturer level, it must be a practice that the devices should have the latest data security and protection software together with frequent up-gradation and continuous training to the hospital staff.

Healthcare institutions must ensure that they have a robust cybersecurity architecture that covers the entire hospital management system together with all radiology and diagnostic devices. They should frequently organise cybersecurity audits to check for any vulnerabilities and loopholes and should immediately plug them. They should also regularly conduct workshops on 'healthy cyber practices' to be followed by all staff members including doctors and management.

On a broader level, the government should also push to introduce a basic cybersecurity curriculum in healthcare education which will give the aspiring medical practitioners first-hand knowledge about computers and cybersecurity, so that doctors, nurses and lab technicians do not violate the cybersecurity guidelines and can become the primary responder to an attack.