



Maintaining SAFE and SECURE Environment in Healthcare



Health services are committed to providing a safe and secure environment for patients, staff and visitors. Hospital security arrangements keep patients, staff and visitors safe from inappropriate behaviour such as violence and aggression.

To keep staff, patients and visitors safe, hospitals use a range of security measures, including the use of CCTV cameras, duress alarms for staff members and electronic access control systems for doorways. Some hospitals also employ security staff.

One of the main reasons the healthcare industry is at a higher risk of data attacks compared to other industries is the type of data collected and stored. Healthcare organizations can have very detailed records of patients that include their name, date of birth, address, social security number, payment account information, and so on.

Healthcare Cybersecurity has become one of the Significant Threats in the Healthcare Industry.

Since healthcare organizations collect such data, it increases the risks of data attacks. Additionally, healthcare data tend to fetch a higher amount on the black markets compared to other types of stolen data.

Current Scenario of Security in Healthcare

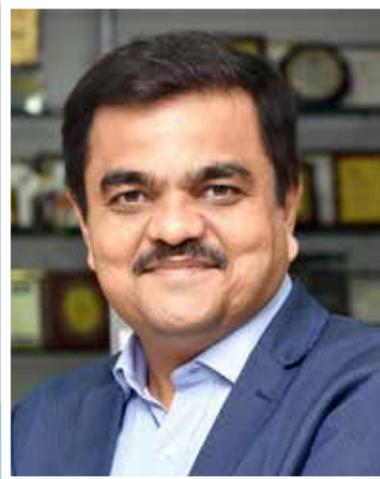
According to Ashish P. Dhakan, MD & CEO, Prama Hikvision India Pvt. Ltd., "At a time when the Indian healthcare sector is combating the second wave of the pandemic, we at Prama Hikvision envisage a pivotal role for

the security industry in providing the innovative security solutions and automation to secure the healthcare facilities. The Indian healthcare industry has been experiencing a surge in physical security breaches in the recent times. The rise in violent incidents in the healthcare facilities has prompted the authorities to spruce up the security management with trained security personnel and effective electronic security systems. The hospital management should consider the security and safety of patients, employee, visitors

and vendors. There are various technologies, which are currently available to ensure security and safety of the healthcare ecosystem.

The typical application scenarios of healthcare facilities include Video Security System, Attendance System, Access Control, Entry and Exit Control, Parking System and Vehicle Surveillance Solutions. The government policies and regulations seek to strengthen health care security and safety at a macro level, health care organizations should focus on compliance, ethics, and risk, and drive awareness throughout the enterprise. The healthcare organizations need to invest in crisis management capabilities that make their physical security management systems resilient. They need to adhere to the physical security best practices and data security guidelines. The compliance of security guidelines will help to protect healthcare ecosystem involving patients, doctors and medical service professionals.”

Aditya Khemka, Managing Director, CP PLUS says, “Electronic health records, also referred to as EHRs, contain a host of sensitive information about patients’ medical histories, making hospital network security a primary IT concern. EHRs make it possible for physicians and other healthcare professionals, as well



Ashish P. Dhakan
MD & CEO,
Prama Hikvision India Pvt. Ltd.



The rise in Violent incidents in the healthcare facilities has prompted the authorities to spruce up the Security Management with Trained security personnel and effective Electronic Security systems.”

as insurance companies, to share essential information. This makes it easier to both coordinate care and facilitate insurance matters. Never before, have medical professionals been able to collaborate in such dynamic ways to meet patients’ needs.

However, the interconnected nature of modern healthcare creates IT security risks - namely that consolidating so much essential

data in a field that nearly all people use makes it a conspicuous mark for hackers and cybercriminals. In fact, the importance of data security in healthcare has never been more pronounced. Now more than ever, medical organizations must be vigilant in establishing safeguards against online threats, which is why it’s imperative to have a solid understanding of the risks and protections available.”

“Much like the previous year, ransomware was one of the healthcare sector’s biggest cybersecurity threats seen in 2020. This spotlights the urgent need for proactive measures. Throughout the past year, the healthcare sector was constantly tested for its resiliency. As on top of the dreadful global pandemic, hackers were and continuously have been trying to take advantage of a weakened workforce and rusty security systems. The healthcare industry has been lagging behind other industries in protecting its main stakeholders, the patients. Henceforth, the time has come when hospitals must invest considerable capital and efforts in protecting their systems. However, this is easier said than done since hospitals are extra-ordinarily technology-saturated, complex organizations with high-end point



complexity and regulatory pressures. Understanding the requirements of the healthcare vertical, CP PLUS has been enabling hospitals with a sense of security through our customized solutions that focus on comprehensively resolving security issues and preventing attacks”, states Khemka.

As per Kaushal Kadakia, Marketing Manager, Matrix Comsec, “At present, healthcare is one of the busiest sectors which is entertaining a lot of crowd on a daily basis. Therefore, the potential risks that the healthcare units face be it hospitals, private clinics and, government hospitals are also higher post COVID-19

intelligent video analytics such as motion detection, intrusion detection, tripwire detection for perimeter security are being deployed. Apart from this, analytics such as missing object detection are being deployed to ensure that there is no pilferage from inventory storerooms. Furthermore, contactless solutions are being deployed to avoid minimum contact. Credentials such as Bluetooth, QR code, Facial Recognition, Palm Vein Recognition are in use to ensure minimum contact. All in all, security deployments are not just being used to govern the premises and prevent casualties but they are being used for the seamless flow of daily operations.”



outbreak. In the context of video surveillance based security, IP-based video surveillance solutions are on the rise as the need for smart monitoring arises. With the healthcare workforce dropping down to almost 50% the healthcare units must implement video surveillance solutions as a part of their smart monitoring of patients to avoid unnecessary contacts. Again, with the requirement to protect physical assets such as the medicines and drug storeroom from any intruders, advanced access control solutions are being deployed which drops the breaches from occurring. Also, video surveillance systems comprising of

As per Sudhindra Holla, Director, Axis Communications, India & SAARC, “Recent developments have created several opportunities as well as challenges leading to disruptions in the pre-conceived norms of business operations and strategies across all industries. While some industries like airlines or hospitality faced the brunt of it, other industries like healthcare and pharmaceuticals rose to prominence.

The role of surveillance in the healthcare sector has thus increased manifold due to some of the potent challenges faced by this industry during the pandemic as well as in

this new normal. With the increasing number of cases, there has been a greater demand for hospitals to turn into specialized COVID care centers. Thus, it is extremely necessary to have an efficient and effective surveillance system not just in terms of perimeter security but also monitoring social distancing norms, staff safety and conduct as well as cybersecurity.”

According to Avinash Trivedi, VP - Business Development, Videonetics Technology Pvt. Ltd., “As the COVID-19 continues to spread throughout the world, hospitals are struggling to provide patient care, ensure the health and safety of medical personnel, and protect vital supplies from theft and pilferage. Hospitals or healthcare facilities are now very much considered as part of ‘Critical Infrastructure’ and utmost consideration is given to safety and security of such premises as well as the workforce and health assets.

Healthcare has been one of the fastest growing industries in terms of revenue and facilities; however, it is equally vulnerable to theft, pilferage, violence, rioting and assault to health workers, false lawsuits, vandalism and other security concerns. Since the beginning of the outbreak, health care providers have been shown more support, solidarity, and gratitude than they ever have. However, recent tragic attacks or harassing healthcare professionals, damaging the facilities etc. have been reported in different parts of the world. Especially, no one can forget bombardment and destruction of a full functioning hospital in Libya that had further reduced the ability of health authorities and aid agencies to prepare for pandemic.

Before the era of pandemic, we have observed an increase in demand for the safety and security of premises, patients, staff, and visitors at healthcare institutions. Hospitals, by their nature, are designed to be open and accessible to the public, which means there is a strong need to have integrated security system to secure health care facilities at various levels.”

As per Parthesh Dhaggal, Founder, Enception, “Healthcare has become

one of India's largest sector, in terms of revenue, manpower and employment. Healthcare comprises hospitals, medical devices, clinical trials, outsourcing, telemedicine, medical tourism, health insurance and medical equipment. The Indian healthcare sector is growing at a brisk pace due to its strengthening coverage, services and increasing expenditure by public as well private players.

Indian healthcare delivery system is categorised into two major components public and private. The Government, i.e., public healthcare system, comprises limited secondary and tertiary care institutions in key cities and focuses on providing basic healthcare facilities in the form of primary healthcare centres (PHCs) in rural areas. The private sector provides majority of secondary, tertiary, and quaternary care institutions with major concentration in metros and tier I and tier II cities.

The hospital industry in India is forecast to increase to Rs. 8.6 trillion (US\$ 132.84 billion) by FY22 from Rs. 4 trillion (US\$ 61.79 billion) in FY17 at a CAGR of 16–17%.

India's competitive advantage also lies in the increased success rate of Indian companies in getting Abbreviated New Drug Application (ANDA) approvals. India also offers



Aditya Khemka
Managing Director,
CP PLUS



Now more than ever, medical organizations must be vigilant in establishing Safeguards against Online Threats, which is why it's imperative to have a solid understanding of the risks and protections available.

vast opportunities in R&D as well as medical tourism.

Automation in the healthcare industry has been benefiting patients, clinicians, support staff, and organizations.

Indian Government aims to increase healthcare spending to 3% of GDP by 2022. M&As jumped a record of 155% over Rs. 7615 cr (US \$ 1.09 bln) in the recent years. The Union Budget 2021-

22 allocated Rs. 2.23 lakh crore for healthcare. The Healthcare Infra has received a big boost.

India's competitive advantage lies in its large pool of well-trained medical professionals. India is also cost competitive compared to its peers in Asia and Western countries. The cost of surgery in India is about one-tenth of that in the US or Western Europe.

In December 2020, a new COVID-19 vaccine delivery digital platform called 'CO-WIN' is being prepared to deliver vaccines. As a beneficiary management tool with different modules, this user-friendly mobile app for recording vaccine data, is in the process of establishing the 'Healthcare Workers' database, which is in an advanced stage across all states/UTs.

As of December 2020, under universal immunization programmes, ~1.54 lakh ANMs (auxiliary nurse midwives) are operating as COVID-19 vaccinators. For further expansion of vaccinators, the government plans to take collaborative effort with states and UTs.

In November 2020, EEPC India and the National Design Institute teamed up to facilitate and improve design and technology for the medical device industry to help meet the increasing



needs of the country's health sector, especially considering the COVID-19 pandemic.

In October 2020, All India Institute of Ayurveda signed a MoU with Amity University for Ayurveda Research. In November 2020, a mobile COVID-19 RT-PCR lab was launched at the Indian Council of Medical Research (ICMR) in New Delhi to strengthen COVID-19 testing services by making COVID-19 testing affordable and more accessible to every citizen.

The number of medical colleges in India increased to >560 in November 2020 from 412 in FY16.

On December 14, 2020, eSanjeevani

have become more conscious towards their healthcare upkeep.

With an automated workflow, approval steps are done in real time. A doctor can use a mobile app to quickly offer approvals for any request, such as a patient discharge.

Similarly, the admission process are being automated to make the process quicker and more reliable. The process often goes through registration, billing, and insurance routes. Automation of different departments in hospitals ensures a seamless coordination of tasks between all departments, without anyone having to leave their desk.

In India hospitals and other healthcare facilities face multiple security and surveillance challenges. These facilities require mission critical security management, but most of the private and government hospitals lack the effective and professional security management systems. In recent times there were many healthcare facilities across India faced violent incidents due to ill-informed patients and relatives. There were cases where many doctors and medical staff were victims of violent attacks. The physical security infrastructure and systems could have helped to detect and deter such incidents."

According to Khemka, "Protecting healthcare information poses the primary concern for healthcare providers as well as governments across the world. As more and more hospitals are digitizing patient health records, there is a clear danger of that information getting compromised or outright stolen. Nonetheless, there are issues that go beyond the typical cyber threats and have the potential to cause severe security breaches. The evolution of ransomware is a sign of what can be expected in coming years, especially for those who keep continuing a reactive cyber posture when it comes to security. The threat landscape for the healthcare sector is struggling with an overabundance of ransomware attacks, a third of which targets the Indian healthcare sector, and a range of phishing campaigns designed to give hackers a foothold onto the network.

Then there are instances where employees of an organization steal property or data to commit other crimes. Surprisingly, the reason insider misuse stands out in the healthcare industry is because of the sheer amount of people who get jobs in the industry for the sole purpose of infiltrating the system and gaining access to patient health information. They typically steal this information to gain access to money or in order to commit tax fraud.

Patient information gets jeopardized also because of the unintentional actions of the hospital staff, which can be quite compromising. A recent Becker's Hospital Review reveals that



telemedicine service of the Health Ministry crossed 1 million (10 lakh) teleconsultations, since its launch, enabling patient-to-doctor consultations from the confines of their home, as well as doctor-to-doctor consultations.

India is a land full of opportunities for players in the medical devices industry. The country has also become one of the leading destinations for high-end diagnostic services with tremendous capital investment for advanced diagnostic facilities, thus catering to a greater proportion of population. Besides, Indian medical service consumers

With new cloud applications, there are many new tools to generate a schedule with much more accuracy and ease. Hospitals are finding a lot of reliefs in making sure their processes are smooth, accurate, and fast."

Major Challenges faced by Hospitals

As per Dhakan, "The key challenges impeding the security management in the healthcare industry are as follows: Noncompliance of physical security norms, lack of security awareness, resource crunch, untrained security personnel, no regular maintenance and upgrade of security systems and integration of security systems on a unified platform.

unintentional staff actions accounted for 12 per cent of security incidents in the healthcare industry. These mistakes can be simple as misplacing a patient's chart, or underperformance by the security system. It also happens when old computers are discarded without removing patient information."

As per Kadakia, "The present challenges post COVID-19 faced by hospitals is maintaining a hygienic environment keeping in mind the safety of everyone. With the outbreak of COVID-19, employee safety along with the patients has parallelly risen on the chart. Also, hospitals need to manage the flow of patients entering in and out of the premises and ensure there is no unnecessary surge in the number of visitors. Further, governing of the premises whether it is kept clean at all times and following the social distancing norms has been added to the list. To add to this, ensuring that people who are walking on the premises are wearing masks and not neglecting the rules. Again, protecting physical assets like laboratories, medical storerooms, and equipment has been another challenge. Any intrusion in such sensitive areas can lead to confidential information getting leaked out of the hospital premises. So, limiting access in such areas is crucial."



Kaushal Kadakia
Marketing Manager,
Matrix Comsec



Credentials such as Bluetooth, QR code, Facial Recognition, Palm Vein Recognition are in use to ensure minimum contact."

According to Trivedi, "The healthcare vertical is both complex and evolving, right from securing their premises to patient and healthcare workers.

From the safety and surveillance perspective, I broadly see various common challenges regardless of any size of healthcare facility:

People Safety: Due to heavy footfalls in such facility, the risk of breaches is more in the form of crimes and break-

ins leading to workplace violence, intrusion, child abduction from incubation centers, etc.

Asset Protection: The theft of expensive and valuable equipments, medicines, personal protective equipments and other supplies are frequent incidents.

Critical Emergency response: The need for streamlined emergency management response protocols for any number of potential scenarios.

Medical Waste Monitoring

Hospital Reputation: False claims and lawsuits against hospitals are a threat to the hospital's reputation and drag hospital administration into legal troubles and losses.

Service Monitoring for overall relationship management between various stakeholders.

Ensuring COVID-19 related protocols related to social distancing, wearing masks and PPEs etc. are adhered to.

In addition, the facility needs to ensure compliance of safety and cleanliness standards by staff including proper cleaning of wards, surgical equipments and maintaining hygiene, etc. The entire staff and visitors of the facility should wear PPE or face masks at designated areas."



As per Dhagga, “The major challenges faced by hospitals include deficient manpower, skills shortage, deficient infrastructure, rising health costs, insufficient funding, cybersecurity, government mandates & regulatory compliances, unmanageable patient load, equivocal quality of services, Providing safety and security to patients and visitor, thefts, internal threats, fire, external market disruption, patient satisfaction, doctor related issues, technological challenges.”

Steps to be taken for a Smart and Safer Healthcare

As per Dhakan, “The healthcare facilities are looking for scalable, cost

useful for the healthcare sector. In addition to high end Artificial Intelligence enabled Deepinview cameras and DeepinMind NVRs, it offers a wide range of IP Cameras, Easy IP 4.0, PanoVu and ColourVu & HD Cameras. Prama Hikvision’s Smart Healthcare Security solutions include intelligent and integrated video security, access control, intrusion alarm, perimeter security, time and attendance and Smart Parking.”

Khemka emphasizes, “The paradox of shared healthcare information is that it simultaneously makes patients safer while also putting them at risk. The larger the network becomes, the more useful it is in providing top-



effective and efficient solutions that can solve security and technology challenges in a sometimes chaotic and stressful environment. They need to implement and deploy systems that can automate simple tasks or integrate into specific security systems that will help the healthcare facility to resolve various security issues.

Hospital security and operation command centers can display multiple cameras on video walls to automate tedious security tasks, improving the safety of their facilities. Prama Hikvision has an extensive range of video security cameras, DVRs, NVRs and solutions that is

quality medical care, but its data also becomes more attractive to criminals.

It has now become critical to ensure that information, communication technology and infrastructure are secure, and a task that has become exponentially more complicated due to the proliferation of mobile devices like smartphones and tablets, healthcare professionals are depending on which more and more in the field. In addition to securing mobile devices, the proliferation of connected devices like medical equipment and other Web-connected elements—the Internet of Things (IoT) — can be particularly weak

security endpoints, and need to be properly secured and updated at all times.

Focusing on cybersecurity should become the top priority for health systems managers everywhere, no matter how small a hospital is. Researches have warned that hackers are still targeting the sector in great force and as can be seen in the news, a resurgence in the number of cases is expected. Although the recent attacks are not entirely new, each brings fresh twists and health and IT executives will need to keep pace moving forward.

“In order to prevent insider misuse, organizations must audit all devices used by staff members. Healthcare providers need to be vigilant in their efforts to monitor access to patient information; the audit can be a reliable way to keep in check who accesses what information. Data loss products like Rescue+ that CP PLUS has launched in partnership with Seagate can be used to protect patient information. It can also be used to show data exfiltration, which occurs when patient data is being transferred outside the organization. At the same time, quality control measures and effective protocol can lessen the impact of unintentional actions or mistakes, which are bound to happen,” comments Khemka.

As per Kadakia, “Healthcare should focus more on automizing the whole patient monitoring to create a smart and safe environment for everyone. With minimum touchpoints for visitors and the workforce, they can automate the whole cycle involving patient treatment and create a safer environment. Also, implementing an advanced access control system can reduce the risks of confidential information or any medicines or drugs being pilferage from the inventory. Limiting the access of employees in certain areas based on user, time, and the zone would lead to smarter security. Video surveillance systems including cognitive analytics would ensure that there are no false alarms.”

According to Trivedi, “Across all the industry segments - the COVID-19 pandemic has created a new set of workplace health and safety practices

that aim to prevent the spread of the virus. As we see the world begin to vaccinate against COVID-19, the medical facilities need to be more vigilant for following protocols as part of such preventive measures. Healthcare facilities have been embracing these new practices, because many of them have met COVID patients and have employees, patients or visitors who may carry the virus and are at high risk of contracting the illness.

This unprecedented pandemic has put every industry across the globe to the test, healthcare brings the forefront of it, requires being more vigilant and should transform its security apparatus from reactive conventional surveillance to AI powered proactive, predictive and intelligent security system so that the facility managers, compliance and security team can respond to critical security situation timely and effectively. The solutions such as monitoring adherence of COVID related protocols, contact tracing of COVID patient, contactless transactions, ensuring cleanliness, hygiene and sanitation, facial recognition with mask/no mask and PPE detection to name a few can greatly help the facility managers. Keeping the complex environment of the healthcare vertical, they require enterprise class solutions.



Sudhindra Holla
Director, Axis Communications,
India and SAARC



With the increasing number of cases, there has been a greater Demand for hospitals to turn into specialized COVID Care Centers.”

Disparate and silo systems on separate platforms have largely gone away in favor of integrated and intelligent unified systems which provides a unified view with greater situational awareness of entire facility and enhances collaborative surveillance.”

As per Dhaggal, “Smart and safe healthcare consist of multiple participants, such as doctors and patients, hospitals, and research

institutions. We need to put in place a system that involves multiple dimensions, including disease prevention and monitoring, diagnosis and treatment, hospital management, health decision-making, and medical research. Information technologies, for example, IoT, mobile Internet, cloud computing, big data, 5G, microelectronics, and artificial intelligence, together with modern biotechnology constitute the cornerstone of smart and safe healthcare.

These technologies are widely used in all aspects of smart healthcare. From the perspective of patients, they can use wearable devices to monitor their health at all times, seek medical assistance through virtual assistants, and use remote homes to implement remote services; from the perspective of doctors, a variety of intelligent clinical decision support systems are used to assist and improve diagnosis.

Doctors can manage medical information through an integrated information platform that includes Laboratory Information Management System, Picture Archiving and Communication Systems (PACS), Electronic Medical Record, and so on. More precise surgery can be achieved through surgical robots and mixed reality technology. From



the perspective of hospitals, radio-frequency identification (RFID) technology can be used to manage personnel materials and the supply chain, using integrated management platforms to collect information and assist decision-making. The use of mobile medical platforms can enhance patients' experiences. From the perspective of scientific research institutions, it is possible to use techniques such as machine learning instead of manual drug screening and to find suitable subjects using big data. Through the use of these technologies, smart healthcare can effectively reduce the cost and risk of medical procedures, improve the

Advanced Security Measures that should be Incorporated Today

As per Dhakan, "The healthcare facilities must take the following advanced security measures: Set up a special command and control center, regular video security footage audit, periodic security and surveillance equipment check-up and maintenance, a robust risk mitigation Plan to address various risk scenarios.

The advanced video analytics software can provide alerts of suspicious activity, such as a person abandoning a bag or backpack, signaling a possible explosive threat. From a clinical perspective, healthcare facilities are opting for video and audio in specialty

Areas, Nurse Station, Corridors, Wards and Rooms. It is vital to have a physical security control Room for unified security management. It is important to monitor parking lots of healthcare facility for efficient vehicle access management. The entrance monitoring should be done at all the time. These solutions are available in two categories of Healthcare facilities: Hospital Solutions and Clinic Solutions. These security systems can help to manage large number of hospital staff, visitors, patients and doctors in the healthcare facility as per health and safety guidelines. The crowd flow solution and social distancing alarm solutions are applicable for visitors lounge and cafeteria to avoid excessive crowding in the healthcare facilities."

As per Khemka, "The dominance of nation-state threat actors attempting to disrupt care operations and steal valuable data related to vaccines and treatments requires ultra-modern and progressive security measures. Regardless of the attack method, similar security efforts can defend against these prominent threats.

Khemka suggests, 'Not knowing where the vulnerabilities lie makes protection against attacks much harder. Conducting risk assessments on a regular basis helps in building a clear understanding of the organization's security issues.

Apart from that, having layered security protocols in place can provide effective protection. So even if an attacker breaks through one layer, they still will not be able to access the protected data. It helps in identifying the attack before it's too late. Just as one installs multiple locking doors to protect property, buildings, and equipment, one should have many layers of defence against electronic intrusions as well. That way, even if a weakness appears in one aspect of the defence system, there will be capable coverage."

As per Kadakia, "In the context of video surveillance, proactive security measures comprising of intelligent video analytics should be incorporated that send real-time notifications in case of any exceptions or any emergency. Further, cognitive



utilization efficiency of medical resources, promote exchanges and cooperation in different regions, push the development of telemedicine and self-service medical care, and ultimately make personalized medical services ubiquitous.

To sum up smart and safe healthcare include Rapid Access/Open Access, Comprehensive Whole-Person/Whole Family Care, Culture of Resiliency and Recovery, Result Oriented Outcomes-Based Care, Quality Value Services, World-Class Customer Service and Staff Engagement and Wellness."

patient rooms to help reduce things like patient falls and IV-pulling, and promote a safer overall environment for patients. The healthcare facility must be fully equipped with security systems to prevent any untoward incident or hazard. The medical professionals and staff must be trained to handle emergency situations like fire hazards, natural calamities, criminal and terrorist acts. They must have an emergency evacuation plan in place.

Prama Hikvision's Smart Healthcare Security Solution covers critical parts of the hospital like Reception, Pharmacy, Doctor's Offices, Patient

analytics ensures that there are no false alarms. Again, important information is not compromised or any sensitive areas such as research labs and medical storerooms are not breached that should be kept in mind. Advance access control systems should be implemented in such areas, to ensure that nothing gets compromised. Finally, to take security to a next level, access control systems should be integrated with IP video surveillance to create a secure environment. The convergence of security systems such as video surveillance and access control not only prevents your hospital from potential breaches but also provides you with evidence against the breach. Hence, in case, something goes missing, you can reclaim the same from the security officials.”

Holla said, “We at Axis Communications, together with our system integrators, have come up with various holistic solutions to support our customers and cater to the ultimate need of the hour.

- **People Counting:** Our People Counting solution has been specifically designed for correctly measuring and swift action to avoid crowds and maintain social distancing which is extremely crucial in all hospitals now. It gives analytics and valuable



Avinash Trivedi
VP - Business Development,
Videonetics Technology Pvt. Ltd.



Disparate and silo Systems on separate platforms have largely gone away in favor of Integrated and Intelligent unified systems which provides a unified view with greater situational awareness of entire facility and enhances collaborative surveillance.”

insights such as – the total number of people in a particular area at a particular time, how they move, where they congregate, and periods of peak occupancy.

This solution has proven to be highly beneficial to the healthcare facilities where extreme caution has to be taken adhering to the measures set by the government for the premises where patients

and people are most vulnerable and exposed to contracting the virus

- **AXIS Occupancy Estimator:** AXIS Occupancy Estimator provides a cost-efficient way to accurately estimate occupancy levels on hospital premises to understand visitor patterns better and how the space is used. It provides real-time data on how many people are present in the premises or in a certain area at a certain time. This data in turn supports operational efficiency to avoid crowding, optimize workforce planning and adhere to the social distancing guidelines.

We have also collaborated with Application Development Partners (ADP) to provide solutions such as Social Distancing solutions, Touch Free solutions, Body Temperature Monitoring solutions, Mask Detection solutions and Touch Free Attendance systems with facial recognition capabilities thus offering a range of holistic solutions to the hospitals and providing them with all the necessary backend support. Audio solutions and Public Announcement solutions are gaining prominence in the larger healthcare facilities hospital,



in the light of the pandemic, to manage crowd and monitor patients for better control and monitoring

- Cybersecurity is another major threat to the healthcare sector as hospitals grapple to protect their databases, especially at this moment. These databases hold sensitive information of all the patients. At Axis Communications, we strongly believe in our As a Swedish-engineered product and solutions company, we have always kept a strongest compliance on all our products. In the current situation, we believe that CCTVs with a

various such facilities, our solution not only creates greater situational awareness but also notifies authorities about potential threats and improves efficiency in day-to-day operations, eventually providing happier, safer, smarter environment to staff, visitors, and patients.

Our Video Analytics based SAJAG Pandemic Management Suite has been efficiently scaled up to act as a true decision support system for security officials at hospitals to not only reduce incidents of infectious disease, in current situation, but also ensuring compliance with government guidelines. SAJAG has been trained with real-time video

Videonetics AI enabled Video Analytics can track the patient's movements in the hospital, monitor doctors and hospital staff visits, ensuring quality care of patients. On the other front, to curb with issues of theft, break-ins, and shoplifting, the video analytics can be installed in critical locations allowing limited access to designated hospital staff.

Vehicle management is also of top priority for keeping a safe hospital today. The Intelligent VMS 3.0 can be integrated with Vehicle Based Surveillance System to provide unified view of monitoring vehicular movement, speeding, wrong way movements etc. This way, we help healthcare facilities in monitoring 'no parking zones', ensuring no congestion for ambulance at the time of entering/exiting the premise, reduce risk and manage transportation more effectively.

Last but not the least, Videonetics Unified Video Computing Platform (UVCP™) provides a freedom to hospital to build one or many control rooms to view real-time alerts, manage them, and respond to them swiftly. Most importantly, Videonetics UVCP™ can play a crucial role in integrating building management system, access control, fire and environmental alarms and video surveillance into a single user-friendly interface. They can use the information being collected by the unified interface to better understand their environment."

As per Dhaggal, "advanced security measures that should be incorporated today are video surveillance, intrusion alarms, smoke detection alarms, facial recognition, and effective access control systems integrated with video surveillance, biometric authentication technologies, firewall technologies, independent health care network, wireless communication technologies, etc.

- Electronic Health Records to protect privacy and confidentiality
- Implementing Endpoint Protection Solutions regardless of whether the attack vector comes

strong compliance policy has a strong competitive advantage and as one of the only few manufacturers, we have our own system-on-chip – ARTPEC Chip, that directly complies with the India's data privacy policy

Timely prevention and security, decreased manual intervention and an efficient surveillance system will help."

According to Trivedi, "We have developed a holistic security and safety solution for hospitals of any size which helps healthcare facilities to streamline their business processes in an efficient manner. Deployed in

data to address real-world challenges pertaining to COVID-19 such as social distancing, queue and crowd management, Masks & PPE detection, ensuring hygiene and cleanliness in the kitchen, to name a few.

Key highlights of Videonetics healthcare solution:

Videonetics Intelligent VMS 3.0 unifies uninterrupted views of camera feeds throughout a facility, thus allowing security operators to keep monitoring every corner of the premise. This also helps hospital management to restrict unwarranted claims and avoid legal troubles.



from the insider threat or external hacking, effectively managing and controlling endpoints is one of the top things healthcare organizations should consider to mitigate these threats

- Installing Robust Cybersecurity
- Data encryption is an efficient means of preventing unauthorized access of sensitive data. Its solutions protect and maintain ownership of data throughout its lifecycle—from the data centre to the endpoint (including mobile devices used by physicians, clinicians, and administrators) and into the cloud
- Encryption is useful to avoid exposure to breaches such as packet sniffing and theft of storage devices. Continuous monitoring through their existing IT security operations team or through managed security service providers offering onsite and offsite solutions
- Inclusion of ICS and medical devices in the overall IT infrastructure and security program

Advanced security measures also include establishing a safety and health management system, building a rapid response system, making sure



Parthesh Dhaggal
Founder,
Enceplon



Security Solutions in Healthcare are growing rapidly.

that employees know and understand safety policies, developing a safety compliance plan, communicating safety information to patients and building practice patient-centered care.

The World Health Organization (WHO) is calling on governments and health care leaders to address persistent threats to the health and safety of health workers and patients.

These involve authentication; access control; audit trails; physical security of communications, computer, and display systems; control of external communications links and access; exercise of software discipline across the organization; system backup and disaster recovery procedures; and system self-assessment and maintenance of technological awareness.

Develop linkages between occupational health and safety, patient safety, quality improvement, and infection prevention and control programmes.

Include health and safety skills in personal and patient safety into education and training programmes for health workers at all levels.

Incorporate requirements for health worker and patient safety in health care licensing and accreditation standards.

- Integrate staff safety and patient safety incident reporting and learning systems.
- Develop integrated metrics of patient safety, health worker safety and quality of care indicators, and integrate with health information system.” 

