How To Prevent Healthcare Security and Data Breaches?

MEDICINE
HEALTH
TREATMENT
DOCTOR
SURVEY
RECIPE
MEDICINE
Contrary to popular belief, Lorem Ipsum is not
It has roots in a piece of classical Latin literature
it over 2000 years old. Richard McClintock

Healthcare Breaches pose serious issues for both Patients and Providers.

Healthcare is in the midst of an exciting transformation. Healthcare facilities are a demanding and complex business to operate and secure. Treating patients is far from the only concern faced by hospitals today.

Hospitals are vulnerable to crime and violence from patients, visitors, and occasionally their own staff members. Therefore, security systems in hospitals must include proactive measures to create and reinforce effective security protocols geared towards accountability, readiness, and responsiveness. To protect the safety of patients, visitors, and staff, hospitals must now take extra efforts to anticipate and prepare for security threats.

Healthcare breaches pose serious issues for both patients and providers. For providers, these incidences affect the trust and relationships they've built with their patients over the years. These breaches could also have legal implications and it's not uncommon for healthcare companies to pay out a large sum of money to affected patients in an effort to mediate the impact of such breaches, meaning knowing how to prevent data breaches can save a great deal in time, money, and headaches.

Without proper attention to detail, a small vulnerability can cause a massive data breach. Security issues need to be resolved and supported as part of a team effort within the hospital organization.

> "The medical Data Theft, patient records pilferage and Privacy Breaches come under the data security and cyber security domain."

Ankush Tandon
Assistant Vice President – Technology
Prama Hikvision India Pvt. Ltd.

Security Threats and Breaches that are taking place in the Health Care Sector

According to Ankush Tandon, Assistant Vice President–Technology, Prama Hikvision India Pvt. Ltd., "In the current scenario, there are two types of security breaches are taking place in the healthcare facilities, one type is connected to a data security breach and the other is related to physical security incidents. The medical data theft, patient records pilferage and privacy breaches come under the data security and cyber security domain. The data security breaches are widely observed in the healthcare sector and can be caused by many different types of incidents, including credential-stealing malware, an insider who either purposefully or accidentally discloses patient data, or lost laptops or other devices.

The physical security threats and breaches include, unauthorized visitors, trespassing in the restricted areas, thefts of material medicine and equipment, violent attacks on doctors and healthcare staff, vandalism inside and outside healthcare facility, infant abduction and unauthorized patient movement."

As per Kaushal Kadakia, Marketing Manager, Matrix Comsec, "Healthcare sectors are the busiest sector, these days - for all the obvious reasons. With a large number of people walking in and out on a daily basis, the risk factors are supremely high. The hospitals and their counterparts need much more than just security. They emphasize on providing satisfactory services by ensuring utmost hygiene and security. With the rapid surge in the number of cases, this task is the most challenging one. Moreover, ensuring that all the safety measures are diligently followed is a matter of concern.

On the other hand, the counterparts are keen on finding a cure to combat the novel virus. With the situation worsening with each passing day, the pressure to find a cure has surged more like a competition. Which, in turn, brings threat to the assets or worse, a scope for data theft. In order to survive this cat-race, the healthcare sectors are forced to act immediately, by introducing effective security solutions."

Parthesh Dhaggal, Founder, Enceplon says, "The security breaches are many that include hacking or IT incidents, theft, loss, unauthorized access or disclosure, improper disposal, and

other unknown types. The breaches occur on computer systems, desktop computers, laptops, e-mail, EHRs, network servers, paper records, and other sources of information.

It was reported that more than 31 million patient records were reached in the first half of 2019, with hacking causing the majority of security incidents and breaching the most patient records, according to the Protenus Breach Barometer. The year 2020 had already seen more than twice the amount of breached records from 2018's total of 15 million.

Human Error, Misuse, Physical Thefts, Hacking is looming concerns.

Malware or malicious software is one of the top causes of data breaches around the world, and today much of it is ransomware. 70.5% of all security incidents involving malware were attributed to ransomware.

Insider misuse and unintentional actions are another set of concern. Healthcare is the only industry in which staff members are behind more data breaches than hackers or other outside threats.

The 2018 Protected Health Information Data Breach Report stated that that most of its data breaches in healthcare were caused by internal actors rather than external ones.

Lack of strict entry control results in anybody getting in and pose security problem.

Therefore, hospitals need to be always vigilant and must leverage tools that allow full visibility into how their data is being accessed, which will help reduce the data breaches."

Preventive Measures

According to Tandon, "The management of healthcare facility should conduct a physical security survey by taking help of a professional consultant. The well integrated physical security management systems (Video Surveillance, Access Control, Intrusion Alarm, Perimeter Security Solutions) at various parts of healthcare facility. The effective security management can be ensured only if the security personnel are trained.

To prevent malware attacks or data security breaches, it is important for every healthcare organisation to get a cyber security audit done of their installations. For data security, hospitals need to follow the guidelines and best practices prescribed by the experts."

As per Kadakia, "Preventive measures that can be taken are:

Ensure Real-Time Safety and Security - Video Surveillance solution for healthcare that provides Crowd Management options and Integration with Access Control to keep track of people entering or going out of the premises. Besides this, with the conditions still worsening, it is important to monitor patients. An advanced option that helps patients to be monitored and also restricts from moving out of their wards is necessary.

With foolproof Access Control Solutions it is possible to deter

intruders. These characteristics ensure perimeter security of the hospital by detecting intruders crossing boundaries and breaking into hospital property. A comprehensive 3-dimensional access control policies are inevitable in such a case, taking care of all combinations of users, location and time.

Instant Notifications - "Prevention is better than cure", they say. Hence, it is of utmost importance to build a vigilant environment, enough to repel intruders. That said it is equally important to keep a close eye on the security, proactively. With a proper video surveillance solution, there are definitive checkpoints that give out instant notifications and alarms in case of exceptions. With intelligent analytics essaying a crucial role, the healthcare sectors can worry less about security.

Quick Investigation - Synchronous and Asynchronous Playback of important events, to prevent questions raised on the hospital reputation. The playback clips also serve as an easy evidence tool for claiming insurance.

Enhanced Customer Service - With the prevailing condition, keeping a constant check on a patient's condition with a bunch of nurses and hospital staff sounds gnarly. On such occasions, the latest solutions break the ice by deploying a mobile application for remote monitoring. This application enables doctors to monitor patients from their mobile or tablet, anywhere and anytime."

Kaushal Kadakia
Marketing Manager,
Matrix Comsec

> "An effective Video Surveillance solution for healthcare provides instant Alerts on Suspicious activities and reconciles any sort of a Threat."

Dhaggal says, "There are many effective preventive measures available to prevent breaches:

By establishing a Risk Mitigation/Incident Response Plan, implementing Security and Privacy Measures, performing PHI Risk Assessment, establishing Security/Privacy Policies and Training, choosing trusted partners, monitoring devices and records, restrict use of personal devices, creating a wireless network for guests, updating IT infrastructure, educating hospital employees, securing the router, installing centralized firewalls and encrypting transmission, restricting access and managing user permissions are essential components of preventing a healthcare data breach.

Enceplon's Remote Health Monitoring Service (RHMS) solution offers 24x7 remote monitoring, timely notifications, alerts healthcare personnel through mobile phones and obviates the need for manual intervention. Moreover, RHMS furnishes regular reports on the status of the devices 'health, captures snapshot of every camera periodically, and stores snapshots for evidence and also saves time and cost. It helps prevent physical thefts in hospitals. Any abnormal activity in the hospital is brought to the notice of its authorities which enables them to take rapid response."

Comprehensive Security Solutions

According to Tandon, "Prama Hikvision's vertical solution team offers a smart healthcare solution to address the security breaches and addressing the evolving risks. The integrated intelligent Video Surveillance, Access Control, Intrusion Alarm and Perimeter security solutions help to mitigate risks and detect threats. In the current pandemic situation, AI enabled end-to-end video security solutions are very helpful. For cyber security and data security breaches regular monitoring, audits and strict adherence to guidelines are the precautionary steps."

As per Kadakia, "An effective video surveillance solution for healthcare provides instant alerts on suspicious activities and reconciles any sort of a

threat. All such places should manage to provide a proactive environment - take extra care and treat the patient well. A solution that aims to offer proactive measures and completely eradicate security threats is a must. Matrix offers a smart IP Video Surveillance solution, which provides both service excellence and security through centralized monitoring and management options.

Furthermore, it is equally important to limit access to specific areas. With the flow of visitors increasing by a manifold, it is equally important to restrict and block predators with effective access control solutions. An absolute Access Control solution will help an organization to safeguard the premises with umpteen numbers of features.

On the other hand, an integration of these two solutions can build a highly secure environment. One would empower the other module to detect potential threats, proactively.”

According to Dhaggal, “There are various security solutions that will be beneficial to the health care segment such as:

- Strategy to prevent breaches
- Effective access control system at important places
- 24x7 monitoring
- Robust surveillance system
- Resetting strong passwords periodically
- Encrypting devices
- Training the staff
- Limiting the access
- Enforcing two or more factor authentication
- Denying or limiting downloading
- Constant monitoring of data and transfers
- Keeping the hardware and software and the systems up to date
- Developing processes for immediately identifying and reporting breaches holding business associates accountable for risk and security assessment
- Regularly checking the vulnerabilities of the systems and subsystems of IT network
- Engaging a data security consultant to give a fresh perspective on existing practices and the need for improvement
- Reviewing arrangements with service providers to ensure that they are subject to appropriate data security obligations
- Creating and promoting a security culture of security in the hospital
- Offsite availability of data backup
- Adopting role-based access”

As per Sudhindra Holla, Director, Axis Communications, India & SAARC, “With the increasing cases of COVID patients in the second lap of the pandemic, it is highly critical to maintain an error free and highly secure database by the

healthcare facilities as it contains a lot of sensitive information making it a hotspot for hackers. Axis Communications, being a Swedish company guarantees a highly secure range of solutions that can be connected through integration. In fact, we are one the few manufacturers to have our own system-on-chip – ARTPEC Chip, that directly complies with the India's data privacy policy. This means that we have absolute control over each and every transistor in our products. This brings in trust and a higher level of cybersecurity for our clients."

System Integration helps in Preventing Breach

According to Tandon, "A good system integration backed by well-planned security design can help in preventing all types of security breaches. The healthcare facilities are a highly sensitive area so system integrator and consultant should mitigate all possible risks with proper project plan and implementation strategy. The insights on the vertical specific requirements and healthcare security solutions are very critical. The system integrator must follow the data security and cyber security guidelines and best practices to protect healthcare facility from the security breaches."

> "The System Integration's involvement is of utmost importance and cannot be overlooked."
>
> **Parthesh Dhaggal**
> Founder,
> Enceplon

> "Malware or malicious software is one of the top causes of data breaches around the world, and today much of it is ransomware."
>
> **Sudhindra Holla**
> Director,
> Axis Communications,
> India and SAARC

As per Kadakia, "Integration with different devices and systems provides overall security to the organization. These include integration with Video Surveillance, Access Control, IP-PBX, fire alarm panels and more!

Moreover, futuristic solutions fully integrate and automate the processes. Notifying proactively or throwing cautions in case of exceptions, activating panels and emergency services in case of an accident - it comes as a complete package that requires no or minimal user involvement."

According to Dhaggal, "System integration is the lifeline of any system including the healthcare security. As it serves as a central coordinator, it prevents or eliminates security breaches in the healthcare industry. Integration of various devices ensures seamless data flow and connectivity and reduces proneness to errors, improving the internal workflow of hospital.

Most hospitals deal with very sensitive information that requires special measures for protection and preservation. By using one system, they can easily build in the security tools necessary to prevent access by unauthorised users. This will help to keep unwanted visitors and hackers out. Ultimately, hospital's patients, visitors, staff and data will be safer and its system more secure.

For example, if access control system is integrated with video surveillance, fire alarm system, biometric reader, patient management software then it helps to prevent any breach as the system automatically alerts any breach-taking place. An integrated system will provide faster access to current developments, figures, and data – ensuring the whole process is simpler and easier to manage. It will attenuate crisis, streamline processes, reduce costs and ensure efficiency. System integration helps in furnishing proper evidence for ready reference to prevent breach in the hospitals.

An Integrated system always helps save time and respond to attempted breaches before they occur. System integration ensures better coordination, cooperation and collaboration with various departments which ultimately lead to Improved security in hospitals."

As per Holla, "The SI's involvement is of utmost importance and cannot be overlooked. Since we are a channel-focused company and rely on our partner/vendor network, their role is critical.

Not only do they help in understanding the key customer requirements, identifying challenges and providing a solution." a&s