COMMENTARY

Security in hospital information systems

Suresh Kumar Balakrishnan and Geetha Govindan

Computer Division, Sree Chitra Tirunal Institute for Medical Sciences & Technology, Thiruvananthapuram 695011, Kerala, India

* *suresh@sctimst.ac.in, geetha@sctimst.ac.in*

Abstract

The Security and Safety of Hospital Information Systems have emerged as a global healthcare challenge. This is because of the progress from the initial independent software applications to a highly interconnected ecosystem with intricate data flow. Data flow not only occurs between medical devices but also flows between the medical devices and the Hospital Information System (HIS). With the introduction of Electronic Medical Records (EMR), the requirement for information sharing has increased for patient care and research. Due to this, HIS managers have to pay special attention to the security and confidentiality of information systems. This paper discusses simple methods that can be utilised to maintain the status of hospital information security in terms of administrative, technical, and physical safeguards in the hospitals.

Citation: Balakrishnan SK, Govindan G (2023) Security in hospital information system, Opn. Med. Sci. Technol. Health, 2023; 1(3): e23022

Received: December 13, 2023

Accepted: December 21, 2023

Published: December 31, 2023

Data Availability Statement: All relevant data are within the manuscript.

Funding: Non declared.

Competing interests: Non declared.

Corresponding Author Address:
Er. Suresh Kumar Balakrishnan,
Engineer G,
Computer Division, Sree Chitra Tirunal Institute for Medical Sciences & Technology,
Thiruvananthapuram 695011, Kerala, India
suresh@sctimst.ac.in

Dr. Geetha Govindan,
Scientist G (Sr. Gr.),
Computer Division, Sree Chitra Tirunal Institute for Medical Sciences & Technology,
Thiruvananthapuram 695011, Kerala, India
geetha@sctimst.ac.in

HIS Infrastructure

Information technology and information software systems are used in health care for quality improvement as well as for expeditious patient care. A robust information system is essential for healthcare professionals to complete their daily tasks efficiently. HIS will also help in establishing communication between different departments/sections inside the Institute and with outside organisations. The security requirement is to protect the data internally and prevent malicious attacks from external sources.

The requirement of health information security must satisfy

1. Availability – Instantly provide health information to the patient and the health care group.
2. Confidentiality – To guarantee that the information inside is not modified nor intercepted and that personal privacy is maintained.
3. Integrity – To guarantee that the health information is not damaged or interfered with and is not used for any other purpose without the patient's consent.

The possible threats in information security are generally classified into three:

1. Natural calamities.
2. Internal events.
3. External events.

Natural calamities

Natural disasters like floods, earthquakes, fires, and explosions can damage Hos-

pital Information Systems. Implementation of remote backup of data based on disaster recovery policy will help to have business continuity without any service breakup. Protection of data and business continuity can be ensured by:

- Implementation of a business continuity plan with proper replication of the entire IT system in safe locations geographically away from the current location.
- Testing the business continuity plan regularly and making sure that the system works without any issues.
- Making a backup policy with a defined data retention period.
- Perform daily backup of all critical data and to keep it in a safe location.

Internal events

According to the Indian Emergency Response Team (CERT-In) report, half of the security breaches involve insiders.

Strict implementation of the authorisation permitted, the authentication for software application access and the segmenting of network access will help to restrict the breaches. Permission for the staff to enter into any software system has to be monitored. Required changes in the permission have to be made, on staff transfer/resignation. Implementing the two-factor authentication with a password and key for login is a secure process in which users provide two different authentication factors to verify themselves. Two-factor authentication methods rely on the user providing a password as a first factor and a second different factor either as a security key number or as a biometric input. This adds an additional layer of security to the authentication process. This makes it harder for the hacker to get into the system, as just knowing the password is not enough to pass the authentication. Software access permissions and access levels need to be authorised only after obtaining requests from the concerned supervisors and need to be provided only for the required period. All activities are to be logged using the audit trials feature.

The following points are to be implemented to minimize the risks.

- Ensuring that the Operating Systems of all servers/ storage and applications software installed are up-to-date and all security patches are applied.
- Installation of a good antivirus software with firewall in all computing units. A proper firewall policy should be implemented by restricting communication.
- Restricting internet access and USB drive connectivity in all patient care systems to avoid data leakage.
- Implementing all security guidelines and advisories provided by Government of India institutes like CERT-In and the National Informatics Centre (NIC).
- Insisting on stronger passwords and insisting on changing the password regularly at periodic intervals.
- Formation of an IT policy and guidelines for the organisation and publishing the same for public view.
- Regular inventory checking for all IT assets
- To limit network connectivity of the medical devices by disabling wireless connectivity.
- Forming a policy for medical device connectivity to HIS.
- Gathering design inputs/ technical details from the original medical equipment manufacturer before connecting the equipment to HIS.
- Restricting unauthorised device connection to the hospital network by implementing security policies in network switches

- Isolating the internet/intranet connectivity for personal devices and hospital network devices
- Providing guest internet access after identity verification and recording the device details.
- All guest and personal connectivity to be filtered and scanned at the firewall level for checking for virus attacks and policy regulations.

With the increase in the advancement of sophisticated technologies, integration between medical equipment and HIS needs special attention. Major equipment manufacturers, by default, have a system-controlled log collection for easy diagnosis from a remote location.

To safely connect the medical equipment and HIS, its remote diagnosis, and log collection, the following points are to be considered:

- A separate network should be created for each company, and access should be restricted between the companies. Communication to be restricted at the switch level and allowed only between specific entities on request.
- Allowing net connection for authorised machines and computers only. Port-level restrictions to be implemented.
- Installing institute-licensed antivirus software with firewall policies in all connected devices for proper communication control and timely updation of antivirus software.
- Ensuring installation of the latest version of the operating system and application software in the medical equipment, which needs connectivity to the institute network.
- Restricting internet connection from medical equipment. (The institute should provide internet access to authorised sites and log all activities if required).
- Restricting remote access from external sources to the medical equipment and providing net connectivity only through the Institute VPN after authorisation. The Medical Equipment Company has to sign an agreement with the Institute for remote access and to ensure the privacy of data kept in the Medical Devices.
- To make a rule for antivirus checking before USB device usage and to allow only permitted USB storage devices and laptops to connect to the local area network.

External Events

Ransomware may affect any of the internal machine connected to the network. Various devices installed in the Data Centre/server room, such as firewalls, network equipment (switches, routers), servers, and devices used in system management, must be protected. All vulnerabilities must be analyzed and effective security protection installed by upgrading the hardware and the server and installing the end-point protection software.

Ransomware, malware, denial of service etc. form the major external threats. Implementing/ updating the latest network security techniques like firewalls, intrusion detection, and prevention systems (IDS/ IPS) and web application firewalls (WAF) are required. Monitoring the inward and outward traffic in the network regularly by the IT professional will help to secure the information system.

The following points are to be considered for protecting the IT assets installed in the Data Centers/ Server Room.

- Implementing the guidelines and advisories from the security agencies from

time to time.
- Updating the software/firmware of all IT communication devices.
- Replacing the IT hardware when there is no support from the original equipment manufacturer.
- Conduct regular IT audits of all communication equipment, servers, and applications.
- Restricting the physical access to the Data Centre / Server Room.
- Restricting the usage of unauthorized devices and USB storage devices for the service of equipment.

Conclusion

Information Security is a process that needs to be continuously assessed. IT Professionals must pay attention to the security alerts made by CERT-IN / NIC of the Government of India and implement and manage the suggested controls.

Regular planning and implementing effective security policies are necessary to overcome weaknesses in information security.

Regular updation of the Operating system, application software, firmware, and antivirus software is mandatory. All unauthorised access to the protected system should be restricted with various policies.

Though a number of methods exist to ensure the security and privacy of health information, developing security policies, implementing access control policies, training users, providing appropriate authorisation, training and supervision of staff, punishing/warning individuals engaged in unauthorised access as well as maintaining equipment with log monitoring are highly recommended.

References

1. Policies and Guidelines for Information Systems and Technology are published on the Internet Website of Sree Chitra Tirunal Institute of Medical Sciences and Technology, Trivandrum. https://www.sctimst.ac.in/resources/IT Policy Approved by the IT Committee Dated 15.03.2016.pdf