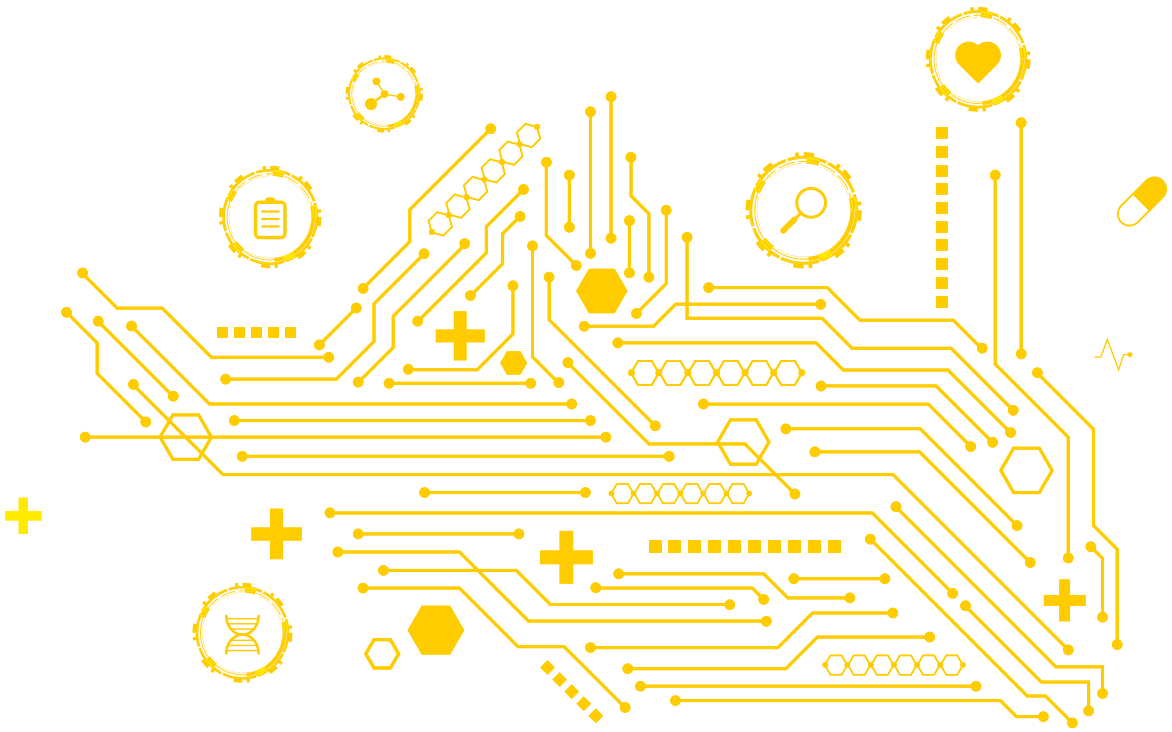
ManageEngine
NetFlow Analyzer

Healthcare IT risk mitigation:
A network-centric approach



Healthcare is one of the fastest growing industries today, thanks to an increased desire for healthy living and the ease of access to excellent medical care. With such an unprecedented surge in demand for medical care, healthcare institutions must seek a strong and robust IT system for efficient management. In fact, today, the IT department is as common as the radiology department in most hospitals. Hospitals rely on IT systems and computer networks to manage the entire patient treatment cycle, from admission to discharge, to the extent that they have come to view the IT department as a value-enhancer, not the “cost center” they were once considered to be.

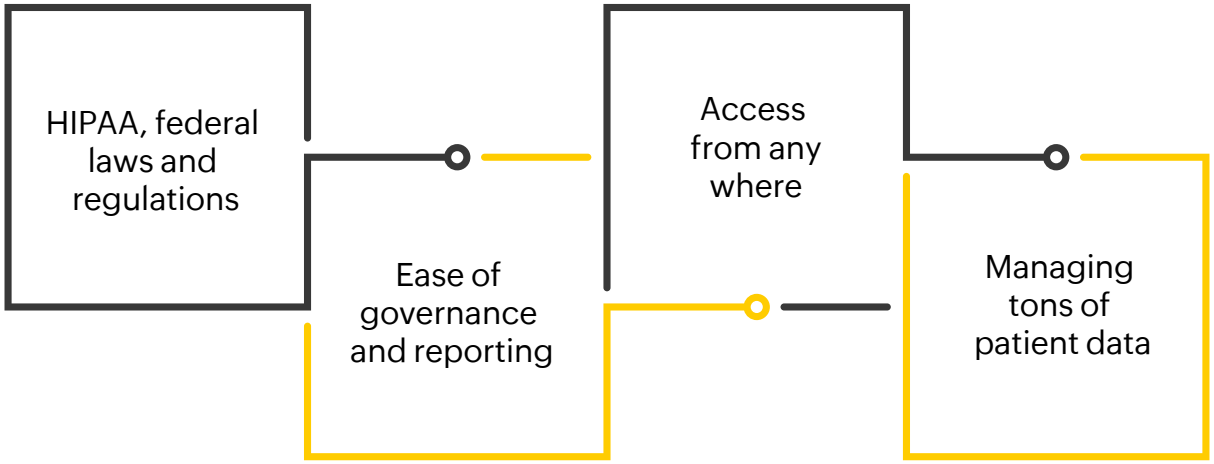
The flip-side to this overarching reliance on IT is that even the slightest glitch in the IT systems could adversely impact their operations. Add to this federal laws like HIPAA that mandate intense scrutiny of IT system security and patient data integrity, and an IT manager's job becomes all the more challenging. This white paper puts forth a solution to overcome the various IT challenges and risks that today's healthcare institutions face.

Healthcare institutions of today

Healthcare institutions come in all sizes, from the basic outpatient-only treatment center down the road to large medical centers in universities and huge community healthcare centers. What they have in common is a strong IT system in place, and even stronger strict federal laws that each institution is governed by; in the case of the large centers, the law is more pronounced, and the fallout of not complying could mean damaging ramifications.

IT spending in healthcare institutions today is like never before, mainly due to the need to manage the health-related information of numerous patients and their medical histories. Also, thanks to information and communication technologies, telemedicine is catching up in a big way, making medical treatment possible from anywhere without the constraints of time and distance.

Prime healthcare IT drivers



Using IT to leverage healthcare delivery

Healthcare software and systems, popularly termed health information systems (HIS), help to automate all the important processes in a healthcare institution. Some examples of this include:

Computerized patient registrations

- A unique medical record number is allocated to each new patient. In the case of returning patients, the number is incremented and reflected in the master patient index.

Allocation of rooms

- For in-patients, an appropriate room can be allocated electronically.

Patient health record maintenance

- All patient health-related information, such as medical history and current health status, is available in electronic records to be accessed by physicians and nurses from anywhere.
- This information can be updated by authorized personnel and viewed by other authorized healthcare staff.

Simplified order management

- A doctor can clearly define the medication to be administered and lay out the frequency and prescription for the nurses to follow.
- Staff can quickly check for any patient allergies, or any lapse in treatment administration can be identified and suitable remedial actions can be taken.

Reduced paper and document overloads

- Picture archiving and communication system (PACS) software enables all documents and images scanned electronically to be stored. This technology is getting cheaper with time, and it has the advantage of providing access to the same document to multiple physicians in various locations at the same time.

An integrated process flow

- With a good IT system in place, it is possible to track the patient's medical history and status at any point in time. Also, billing gets easier, as each treatment given to the patient—lab tests, radiology scans, medicine, upgraded rooms—can all be accounted for and billed for as a whole. It is also much easier to process claims from insurance agencies with such a workflow.

Compliance with HIPAA and other federal guidelines

- The Health Insurance Portability and Accountability Act (HIPAA) and other federal laws were the straw that broke the camel's back and made hospital systems take to IT in a big way. With growing emphasis on maintaining electronic medical records and ensuring the integrity and security of patient data from unprivileged access, IT is the only way forward.

The catch

As can be seen from the number of benefits above, healthcare institutions with an IT system in place stand to gain much more than the upfront spending they incur. Yet, one major caveat here is the extreme reliance on IT systems, which in turn rely on nebulous computer networks.

What this means for healthcare centers is that a single network mishap could render the IT system unusable—and with it goes away the access to patient information and medication instructions.

Also, with the widespread use of electronics for communication and entertainment purposes, hospital networks are always under threat of being abused for purposes that are not within the purview of patient treatment. Such a phenomenon could unnecessarily burden the network, stripping the availability of bandwidth for a much more critical application.

A network disaster could pose a serious risk to the reputation and even the existence of the healthcare institution. This could include:

- Failure of a network element that goes unnoticed
- Loss of access to IT applications (HIS)
- Lack of enough bandwidth for healthcare-related activities
- Unauthorized intrusions into the network and virus attacks that could spell disaster for medical systems

So, attempts to mitigate network risks by having mechanisms ready to combat a network disaster are well in order.

A case in point

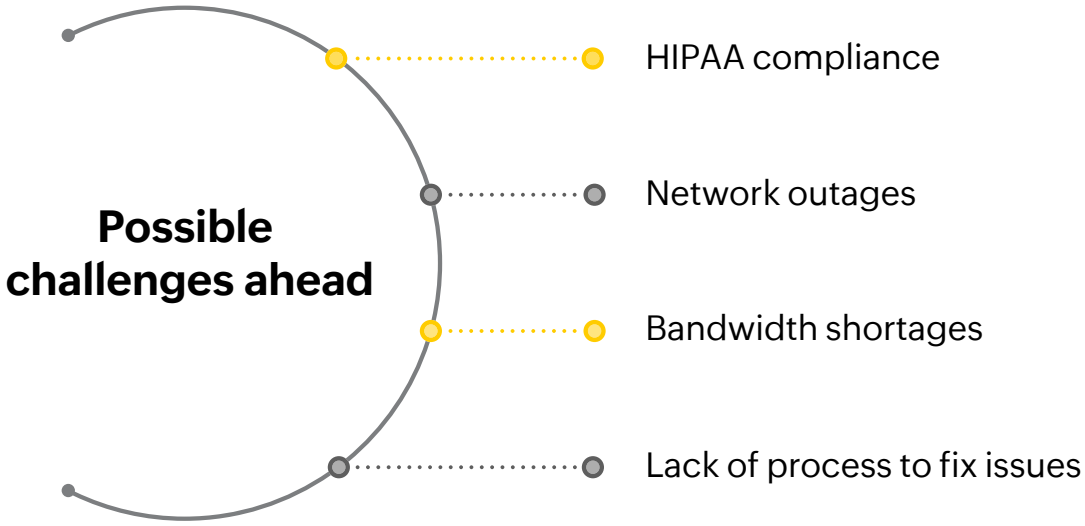
Consider the case of a large community medical center that has 5,000 employees and 60 distinct business units. To achieve high levels of service delivery and efficiency, the medical center deploys a sophisticated HIS that spans its entire campus.

Its infrastructure includes:

- A comprehensive HIS to automate the whole process flow, including the capability to digitize patient records in the form of a PACS

- A high-speed bandwidth line connecting the entire campus
- VoIP systems to enable easy and cost-effective communication
- Access to wireless internet anywhere on the campus through access points

Risk assessment: The key points to consider



As the medical center is heavily reliant on IT and computer networks, ensuring remote data access and network connectivity is critical for the smooth functioning of the whole enterprise. The network administrator or CIO has to anticipate the possible problems that may crop up and disrupt the smooth functioning of the healthcare delivery process. Possible challenges include:

The network going down and access to computers and printer systems taking a hit

- Physicians can't access patient health information, medication and surgical orders get disrupted, and administrative staff can't access data relating to discharge and billing.
- There are also heavy losses due to mistakes that happen in the event of missing data access.

Network bandwidth being wasted on non-critical applications, like streaming videos

- Due to unwanted applications eating up the bandwidth, vital applications like the PACS don't have enough bandwidth to support physician access from anywhere instantly.
- Consequently, access to the HIS takes a hit.

Unprivileged access to patient records, violating HIPAA

- The healthcare center violates HIPAA by not ensuring adequate protection to patient data. In the event of any such scenario, the hospital is expected to be capable of reporting all these details to the proper parties.
- Losses include painful legal hassles, defamatory suits, and lost brand equity.

Very high mean time to repair (MTTR)

- Any network-dependent enterprise should have procedures and processes in place that facilitate quick fixture of problems in the network. This is all the more important in a sensitive industry like healthcare—being able to fix and troubleshoot problems faster could mean the difference between life and death.
- The system should be able to assign responsibility to personnel to fix problems and to track the progress of the resolution.

Risk mitigation

Having assessed the potential risks that an enterprise is vulnerable to, it is vital to address them effectively before they can cause problems.

The challenge (perceived risk)	The solution (risk mitigation mechanism)
1. Monitor networks and proactively thwart any possible network failures.	Have good network monitoring software that can inspect your entire network and give meaningful, in-depth reports to help wade through the problems.
2. Monitor network bandwidth usage and ensure high bandwidth availability for critical applications.	Have a strong WAN monitoring solution that can monitor the entire network's bandwidth and all network traffic. It's also beneficial to get reports on who the top talkers are, what applications are eating up the maximum bandwidth, when the bandwidth peaks, and the

	bandwidth usage pattern over the last couple of months. More importantly, such information can help decide how to perform capacity planning.
3. Log all access to the HIS system and patient records.	Have a strong log analyzer solution that can capture and store logs with information on all accesses, such as successful or failed attempts to access the HIS. It should also be able to report on the stored logs and provide actionable decisions, and generate reports on HIPAA compliance.
4. Reduce the MTTR, and in case of any event or disaster, have a strong disaster recovery process in place.	Have sound help desk management software that can help assign ownership to individuals in charge of resolving issues and track the progress of the issue for quick resolution.

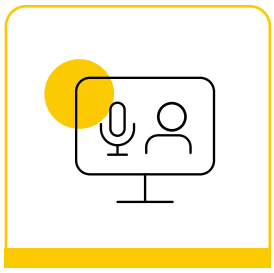
NetFlow Analyzer as a network traffic monitoring tool

ManageEngine NetFlow Analyzer is a tool that harnesses the NetFlow data export from routers and switches to analyze and report on vital parameters, like who the top talkers are, which applications are consuming the maximum bandwidth, and whether there has been any network attack or unscrupulous access attempts. You can also use this tool to drill down to find the origin of a persisting network issue with raw data reports and deep packet inspection.

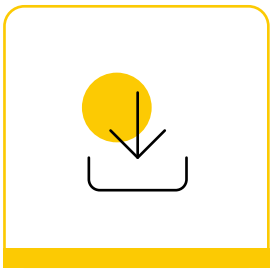
Armed with this information and with provisions to be proactively alerted about any threshold violations, you can stay proactive and prepared when it comes to your healthcare network.

Explore more about NetFlow Analyzer

Get Price Quote



Request Demo



Download Free Trial