Syteca

Case Study

A US Hospital Ensures Data Security and HIPAA Compliance with Syteca

The challenge

Our customer is a general hospital that needed to establish robust security for patient data in order to meet HIPAA requirements. Specifically, they highlighted the following needs:

- **Ensure that staff handles patients' data securely**
- **Prevent the loss of patients' sensitive data**
- **Collect evidence in case of an incident**
- **Secure data stored on corporate servers**

It was essential for our customer to monitor how employees handle protected health information (PHI) and work with core hospital applications. They also wanted to keep an eye on privileged users to eliminate the risk of their stealing data, changing cybersecurity settings, or compromising corporate networks.

Another challenge for our customer was to make sure they could retrieve incident-related data in case of a security incident. They required this data to provide relevant reports and evidence according to HIPAA requirements.

And since our customer stores their most sensitive data on servers, they also needed to monitor the actions of users when accessing those servers.

After exploring several user activity monitoring and compliance solutions, our customer tried the Syteca platform. They appreciated its user-friendly interface, advanced features, and variety of deployment options, so they decided to adopt it.

The customer

Organization type: Healthcare

Location: United States

Market: Global

Must comply with: HIPAA

Pending issue: Monitor users' access to PHI, hospital software, and corporate servers.

Customer’s objectives	Results achieved	Our offering
Ensure that staff handles patients’ data securely	Complete visibility into employees’ actions with patients’ data	Continuous user activity monitoring
	Insights into how users with elevated access rights handle patients’ data	Extensive monitoring of privileged users’ activity
Prevent loss of patients’ sensitive data	Immediate detection of potential incidents	Abnormal user activity detection
	Ability to stop insider threat incidents in real time	Instant alerts on suspicious actions and real-time user session view
	Limited access to sensitive data	Ability to grant access to sensitive data only to those employees who need it for work
Collect evidence in case of an incident	Reports on security incidents that comply with HIPAA requirements	Customizable and scheduled reports
	Proof of users’ malicious actions in the form of employees’ session records	Exporting of full monitored user sessions or session fragments
Secure data stored on corporate servers	Ability to prevent unauthorized access to sensitive data on servers and ensure its security	Monitoring of users’ access to servers and tracking of user activity

The results

After deploying Syteca, our customer successfully achieved HIPAA compliance thanks to PHI data protection and employee monitoring. In particular, they achieved:

- ✓ Complete visibility into employees' actions with patients' data
- ✓ Insights into how users with elevated access rights handle patients' data
- ✓ Immediate detection of potential incidents
- ✓ The ability to stop insider threat incidents in real time
- ✓ Limited access to sensitive data
- ✓ Reports on security incidents that comply with HIPAA requirements
- ✓ Proof of users' malicious actions in the form of employees' session records
- ✓ The ability to prevent unauthorized access to sensitive data on servers and ensure its safety

Additionally, our customer enhanced their data security by leveraging Syteca's USB device management functionality. Now, they can monitor and control all connected devices and set rules for blocking the connection of prohibited device types.

How we did it

The Syteca platform helped our customer achieve their goals by providing a set of helpful features including:

Continuous user activity monitoring

The customer can analyze gathered monitoring data to make sure staff securely handles both PHI and healthcare software, which is required by HIPAA.

Extensive monitoring of privileged user activity

Our customer can also check whether privileged users handle patients' data securely. They can keep track of actions performed by users with elevated access rights, including system administrators.

Abnormal user activity detection

The customer can detect a potential incident before it turns into a breach. This is possible thanks to an AI-driven UEBA module that establishes baseline user behavior and detects abnormal user activity. This also allows our customer to identify compromised accounts.

Instant alerts on suspicious actions and a real-time user session view

Security officers receive immediate notifications when a potential danger is detected. Then, they can view the user session in real time to check whether an employee has violated cybersecurity rules and respond accordingly. This also allows security officers to detect careless workers who neglect cybersecurity policies.

The ability to grant access to sensitive data only to those employees who need it for work

To enhance the security of PHI and minimize the chance of data leaks, our customer adopted efficient access management functionality. Now, our customer's employees can only access data needed to carry out their work.

Customizable and scheduled reports

Our customer now receives convenient reports automatically on a desired schedule with specified monitoring data. In case of a security incident, they can retrieve incident-related data in a few clicks and provide relevant reports according to HIPAA requirements.

Ability to export a full monitored session or session fragments

Our customer can now provide evidence for incident investigations by exporting a full monitored session or a session fragment in a protected format suitable for forensic activities.

Ability to monitor user access to servers and track user activity

After installing Syteca on a jump server, our customer secured the sensitive data stored on their servers by monitoring users' access to servers and the way users handle data on them.

With the Syteca platform, the hospital monitors unlimited amounts of terminal user sessions on ten corporate servers. Our customer is satisfied with the way Syteca helps them protect sensitive data, audit privileged access, and comply with HIPAA requirements.

See how Syteca can secure your data by requesting a free demo!

www.syteca.com Syteca info@syteca.com