



patient privacy & hipaa ACTIVITY MONITOR



patient privacy & hipaa

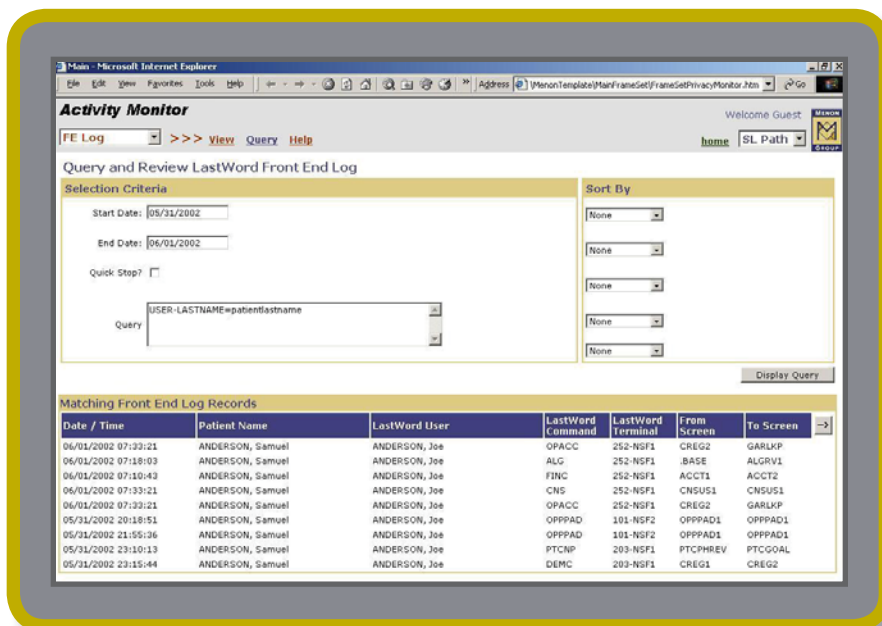
understand how patient information is accessed and used

The *Activity Monitor*™ application from The Menon Group complements enterprise-wide security applications by allowing a deeper level of analysis. In light of HIPAA requirements, *Activity Monitor* helps organizations manage and enforce patient privacy standards by combining detailed information from the clinical system with sophisticated analysis capabilities.

The key to *Activity Monitor* is that it adds to the audit review features of the GE Centricity® Enterprise system to help security personnel analyze detailed information about users, patient records accessed and activities performed. It's flexible enough to accommodate a wide range of queries. For example, organizations can use *Activity Monitor* to monitor certain patients and send an email or page to specified staff when an unauthorized user accesses one of those records. *Activity Monitor* can alert a system operator if there are three successive failed logon attempts from the same workstation. If a patient wants to know who has accessed their online record, *Activity Monitor* can provide that information. For thorough retrospective analysis, *Activity Monitor* can perform specific queries and download the results to a PC. *Activity Monitor* supports an organization's multitiered approach to monitoring system use for patient privacy standards, including, 1) Proactively monitoring access to the records of specific patient populations and alerting specified staff; 2) Taking random samples across the user population to analyze for potential breaches; 3) Looking for patterns of access that might indicate a breach; and 4) Researching a specific incident in order to take swift and appropriate action.

KEY FEATURES

- **know immediately about a breach.** Appropriate staff can be notified immediately via email or pager of failed logon attempts or unauthorized access to the record of a specifically monitored patient, such as a VIP or an employee, so that action can be taken right away.
- **gather pertinent details.** Thorough analysis is made possible using details provided by *Activity Monitor* about



Use *Activity Monitor*'s powerful query capabilities to monitor your Centricity Enterprise system for potential breaches, such as a user accessing the records of a patient who may be a relative. This level of analysis helps you comply with HIPAA and organizational standards.

the user, such as title and department; the patient, such as discharge date and registration flags; and the activities performed, such as commands used.

- **download information to other applications.** The security team can download the results of *Activity Monitor* queries as a delimited file to workstation-based applications, such as Microsoft Excel, for further analysis.
- **use powerful search capabilities.** *Activity Monitor* provides powerful search and analysis using Boolean and regular expression searches.
- **define, save and run queries.** Extensive query capabilities enable staff to assess the appropriateness of access to patient records or be alerted immediately of potential breaches. Queries can be saved and run automatically as part of routine monitoring procedures.
- **respond to patient requests.** *Activity Monitor* helps organizations respond efficiently to patient requests related to HIPAA provisions. For example, if a patient wants to know every organization employee who accessed his or her online medical record in Centricity Enterprise, *Activity Monitor* can easily provide that information.
- **analyze system activity.** Staff can analyze the Front End (FE) and ERS logs for today or prior days to understand system activity.

SAMPLE ACTIVITY MONITOR QUERIES

These sample queries might be used for routine monitoring or by an analyst in response to a specific situation:

- **which patients did users in each department access?**
By distributing lists to department managers of patient records accessed by each of their staff, managers can look for patterns, such as a user looking at records for patients outside the department, and then take appropriate action.
- **did this user access records for patients related to them?** By comparing the user's last name with the last names of patients he or she accessed, the analyst can look for matches. This search can be extended to look for instances where the user might be the patient's spouse, next of kin or alternate contact.
- **has there been inappropriate access to inactive patients?** Looking for users who accessed patient records with no open accounts and no recent visits might indicate inappropriate access.

SYSTEM REQUIREMENTS

- Guardian® operating system version D30 or higher.
- Microsoft Internet Explorer version 6.0.
- Available for all Centricity Enterprise (Carecast/LastWord) versions.

how customers use *activity monitor*

- **audit access to patient information.**
If a patient raises concerns at **Saint Francis Hospital and Medical Center** in Hartford, Conn., about who accessed their medical information in Centricity Enterprise, the security staff can quickly provide a very detailed report using *Activity Monitor*.
- **track physician utilization.** **Saint Francis** also uses *Activity Monitor* in conjunction with other reports to track remote access by physicians in their offices or homes to support efforts to encourage physician utilization of Centricity Enterprise.

