AKERSHUS UNIVERSITY HOSPITAL

Safeguarding patient privacy with security information and event management

“Patient safety is our primary concern and we take the security of their private files very seriously so we needed a tool to ensure medical staff would not abuse their access privileges. RSA® enVision® was chosen by Akershus University Hospital as the preferred tool to accelerate identification of suspicious activity whether it is intentional or accidental.”

TOR OTTERSEN, SENIOR ADVISOR AT THE DIRECTORATE OF HEALTH

One of four hospitals affiliated with the University of Oslo, Akershus University Hospital (Ahus), is situated in the Lørenskog municipality in the southeast of Norway. It employs 4,000 and has more than 700 beds. Its main building, opened in November 2008, makes the site one of the most modern, both technologically and architecturally, in Europe.

KEY REQUIREMENTS

The Ministry of Health and Care Services (HOD) is dedicated to providing equal access to high-quality health and medical care for the population of Norway, representing just under five million people. Its subsidiary, the Directorate of Health, is responsible for defining government strategies and policies for delivering these services nationwide.

Since 1995, a series of new European regulations has been introduced to protect the security and privacy of personal data held by corporations and public bodies, particularly concerning the logging of access to sensitive information. Keen to ensure its hospitals and clinics comply, the Directorate of Health developed a Code of Conduct specific to data protection in organizations wishing to connect to the national network.

Tor Ottersen, Senior Advisor at the Directorate of Health, explains: “Of course patient safety is our primary concern and we take the security of their private files very seriously. We also need to ensure medical staff do not abuse their access privileges for their own benefit. So Norway’s hospitals need a failsafe way of monitoring all access to patient records and accelerating identification of suspicious activity whether it is intentional or accidental.”
SOLUTION

An audit by the Norwegian Data Inspectorate, the government agency overseeing data-security compliance, found that Akershus University Hospital did not adequately monitor access to patient data or create needed audit trails. Addressing this issue was the hospital’s first priority for meeting regulatory requirements.

Ellef Mørk, Chief Information and Security Officer at Akershus University Hospital, adds: “Just as important as compliance for us, though, was that our patients felt confident in our ability to keep their personal data out of the wrong hands. We needed to control what each member of staff was allowed to access and know when breaches were attempted so we could investigate them. With 1.4 million access instances to our system every month, we needed a strong log-monitoring tool to identify the small proportion that was not authorized.”

After reviewing a number of proposals, the hospital chose a traceability solution offered by RSA, The Security Division of EMC. RSA proposed a solution based on the RSA enVision platform to collect, analyze, and manage all log data.

The hospital IT team worked with RSA to create a set of correlation rules for tracking access to the system, which assigned each staff member the appropriate level of access. It was then deployed so that its effectiveness and scalability could be tested before rollout to further sites.

RSA SecurID® technologies also provide further security by controlling access to patient records over the hospital VPN. Two-factor authentication, based on something a user knows (a password or PIN) and something he or she has (an authenticator), ensures information shared over email meets legal security requirements.

RESULTS

The security information and event management (SIEM) platform enabled immediate compliance with the Code of Conduct.

As the new system is based upon rules pre-defined by the Directorate and hospital management, both can be confident that requirements are met consistently with no risk of human error.

The automation also saves time. “When we suspected unauthorized access to the system, in the past it could take up to five days to get the log report,” comments Mørk. “This meant time spent tracking down possible breaches, often without knowing whether they were genuine. RSA enVision can now accelerate the process, alerting us automatically to any unauthorized activity and providing all details immediately. We save a huge amount of time and if we do have a breach we have the data to prove it.”

With more aspects of the Code of Conduct expected to become law, the Directorate is now planning to extend the solution to other hospitals and healthcare systems and is assessing the potential of other RSA technologies.

“We expect to develop a solution for SIEM and log management that can be a blueprint for the healthcare sector in Norway and look forward to continuing our work with RSA to achieve this,” concludes Mørk.