Security Solutions for HIPAA Compliance

www.currentware.com | 613-368-4300 | info@currentware.com

In today's digital and mobile age, the healthcare sector is susceptible to increasing vulnerabilities of exposing confidential patient files. With the dissemination of data via the information "super highway" and mobile communication devices, the incidences of data loss through security breaches continues to be a growing risk for medical facilities.

To safe guard the privacy of patient information, the healthcare sector in the US is obliged to comply with the guidelines under the Health Insurance Portability and Accountability Act (HIPAA).

CurrentWare offers a range of solutions to help healthcare organizations address HIPAA compliance security standards http://www.currentware.com/practice-ready-hipaa-compliance/

BrowseReporter

Monitor Internet usage, by tracking and reporting on the websites visited and duration of visits by the healthcare staff. Identify users that are frequently visiting sites that may compromise patient information or infect your network.

Real Time Monitoring

Accurate real time monitoring of Internet activity on a per employee or per computer basis. Meticulous recording of all employee Internet activity.

Bandwidth Tracking

Capture and instantly analyze bandwidth usage, to realize bottlenecks and detect trends of suspicious usage of bandwidth.

Screenshot Capture

Should you have suspicions of an employee or any activity on specific computers, trigger a screenshot of the desktop, to record any proof of illicit behaviour that could damage the organization.

Inclusive Reporting

Intuitive report generator allows you to instantly generate reports at the executive summary level to the detail level. Reports are easy to follow, facilitating rapid identification of suspicious Internet activity.

Email Reports Automatically

Schedule reports to be automatically emailed to the managers on a daily, weekly or monthly basis.

Offsite Monitoring

Computers or laptops that are typically used offsite, such as in ambulances, can be assured the same level of Internet monitoring as the computers that are onsite. Monitoring of offsite systems is not compromised.

BrowseControl

Protect against Internet threats, by blocking and filtering websites not related to the medical facility. Enforce Internet restriction policies for HIPAA compliance. Improve staff productivity and mitigate security threats to your network and healthcare data.

Whitelist & Blacklist Sites

Reduce Internet threats and infections by restricting access to medical related sites only, by employing the Allowed List and Blocked List feature.

URL Category Filtering

Choose from over 100 URL Categories to instantly block thousands of sites within a Category. Restricting access to questionable sites, reduces the risk of users frequenting malicious sites that could be hosted by hackers, waiting to penetrate a vulnerable medical practice.

Block Downloading of Files

Restrict users from downloading files that could inadvertently result in compromising the company network. Preventing users from downloading music and video files limits the hogging of the corporate bandwidth and reduces staff distractions.

Block Suspicious or Time Wasting Apps

Increase employee productivity by blocking time wasting applications such as online chats and games.

Offsite Filtering

Laptops used by mobile medical workers can be subject to the same Internet policies as those onsite. This mitigates the risk of Internet misuse by offsite employees as well.

AccessPatrol

With the influx of mobile storage devices such as USB devices and smartphones, stealing confidential patient data can be achieved quite transparently without the knowledge of authorities.

AccessPatrol provides comprehensive endpoint security to prevent theft of patient records:

Enforce selective data access

Implement access privileges: read only, read and write, or no access to patient data files.

Whitelist endpoints

Totally block access to all endpoints. Or allow access to authorized endpoint devices such as USBs, using the AccessPatrol Allowed List

Monitor Access

Identify the time and duration of use of allowed and blocked devices. In times of suspicious activity, identify which computers were susceptible to access by blocked endpoints.

Comprehensive Reporting

Inclusive reporting ensures speedy identification of abusive use of endpoint devices.

Offsite Management

Endpoint security polices will be maintained, even if the computer or laptop is used offsite.

CurrentWare is a global leader of Internet and Endpoint Security solutions. We are committed to delivering products with the immediate benefits of increasing productivity, enhancing security and improving cost savings. CurrentWare products are intuitive to manage and focus on solving real world computing challenges.

CurrentWare offices are located in the US, Canada, Australia and Asia. We have a master distributor in the UK that distributes our products to the European, Middle-East and African markets. We are focused to meet the diverse needs of today's technology demands globally.

To learn more about controlling and monitoring your employee's Internet access, visit our website at http://www.currentware.com

CurrentWare's Internet Management Solutions

Icon Set by Paomedia