The Medical Standards Regulatory Agency responsible for establishing and maintaining medical standards as well as providing accreditation to medical schools and practitioners in a major South Asian country selected GhangorCloud Information Security Enforcer (ISE) solution. The Agency also monitors medical practices to ensure the most current standards of medicine are taught and practiced. Additionally, it establishes criteria for recognition of medical degrees from other countries.

The Agency needed data leak protection mechanisms to safeguard sensitive data regarding testing content, test scores, accreditation status and physician information. The Agency deployed GhangorCloud’s Information Security Enforcer (ISE) to automatically identify, protect and monitor sensitive data, block unauthorized transfers and/or downloads of restricted information (including PII, PCI, test information, medical professionals’ data and accreditation related information).

The Agency had several key requirements from a DLP solution including: (a) Real-time monitoring dashboard for instantaneous reporting of any violation of the controlled data, (b) Automated identification and protection of controlled data including PII, PCI, Medical Practitioner’s Accreditation Information, Medical Curriculum Standards, Medical Standards and Guidelines, etc., (c) Easy to use interface for the Agency’s staff, (d) Minimal Deployment effort and minimal on-going human intervention.

The Agency required a low maintenance solution, as they were not able to devote large numbers of resources to installing and maintaining a DLP system. A key aspect of maintenance is the ability to easily add and change access rights for members of the Agency as it grows. Since the Agency does not have a large IT staff, they also needed a solution which would automatically identify and protect restricted information without any tedious and costly document tagging or fingerprinting process. The Agency also needed to maintain forensic records of any potential data exfiltration attempts. The ability to quickly generate actionable reports to address any incident of data privacy violation was another key requirement.

The Agency has multiple offices distributed across a large geographic area. This required monitoring of a variety of communication protocols with distributed Policy Enforcement for each site and a Centralized Control.
How to get started:
GhangorCloud understands that every enterprise has its own unique data security needs. GhangorCloud’s team of Data Loss Prevention experts and its Value-Added Distributors will work with you to understand your unique data security requirements and priorities.

Please contact GhangorCloud to get started: email info@GhangorCloud.com.