Protecting Personal Health Information on Premise and in Azure

The Challenge

A large internationally recognized health care provider needed to secure patient records and comply with the federally mandated Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health act (HITECH) regulations for a large hybrid cloud application used by thousands of physicians, nurses and support staff.

The organization needed to address the Protected Health Information (PHI) privacy regulations requiring that access to personally identifiable health information be audited and explicitly controlled. Because the healthcare provider's business intelligence and other applications used generic database user IDs, monitoring at the database level alone lost the user ID. Auditors could not correlate the actual user with the sensitive data accessed. This prevented the provider from meeting a critical compliance requirement for auditing and controlling access and masking sensitive by users and roles.

The Solution

After reviewing a wide range of data protection and compliance solutions, the healthcare provider selected Teleran's solution. It provided compliance auditing and data access policy controls that enabled the provider to protect sensitive patient health information both on premise and in Azure by applying policies at the individual user level independent of the applications and databases.

Teleran's Identity Persistence™ capability ensured that each user was identified, his or her data access audited and their access appropriately controlled. With Teleran, the provider was able to expand the access to a broader range of healthcare staff across their network of clinics with confidence that their patient data was protected and HIPAA PHI requirements were quickly and cost effectively met.

BENEFITS DELIVERED

Lowered compliance costs and risk with packaged HIPAA audit reporting and data masking and access controls

Identity Persistence™ correlated database SQL transactions despite connection pooling, ensuring data protection policies were enforced

Delivered real-time sensitive data masking access controls automatically adapted to each unique application and user

Applications integration enabled audit reporting at user, applications and database layers

Identified and alerted to suspicious user behavior for immediate response