eBOOK

Overcoming the Complexities of Securing Health Data

SailPoint

The healthcare industry is rapidly evolving. Among the many significant industry changes are the ongoing mergers and acquisitions, the proliferation of accountable care organizations, and the integration of multiple health IT vendors into day-to-day hospital operations. Couple these changes with the fact that more patients are accessing their healthcare records electronically, and providers must cope with growing demand for sharing highly-sensitive patient data between organizations and individuals. However, with increasing demand comes increasing risk, particularly with information security and regulatory compliance. To ensure timely and proper access to applications, files and data, providers must navigate through a myriad of hurdles.

Multiple Authoritative Sources

Many provider organizations have multiple authoritative sources including human resource applications (HR), electronic health record systems (EHRs), learning management applications (LMS) and physician credentialing applications often referred to as MSOW. These and other systems and applications are deemed by the provider organization as the true source for defining user identity and access rights. However, having to manage multiple identity sources and their access rights creates difficulty in ensuring consistent execution of policies and resource optimization.

Diverse User Population

Within the healthcare-provider setting, there is typically a diverse and transient population that requires access to health information as part of their regular workflow. This may include hospitalists, employed staff, contracted physicians, students, volunteers, vendors, etc. Ensuring the right people have the right access at the right time is a daunting task. However, the consequences for not doing so can create security gaps with serious financial and operational repercussions.

Multiple Roles (Personas)

Personas – individual roles or bundles of entitlements – help to build an identity by defining the different ways in which an individual engages a provider organization. In some cases, an identity may have multiple personas. Consider the healthcare provider ecosystem where physicians, nurses, professors, researchers, contractors, volunteers and students are just a handful of job functions that may be present in one hospital. Yet many individuals can perform more than one function during any given day. To illustrate, a unit clerk in the emergency department may also be a nursing student who is doing a clinical rotation in the ICU. A physician may have an outpatient clinic in the morning and perform research work in the afternoon. Also, nurses may float between departments. To complicate matters, many of these functions can be transient.

Disparate Processes

User access is not always managed by any single department or team. At the same time, it is often managed through functionality native to the specific application. This creates disparity in processes that lead to security gaps and unnecessary burden on IT administrators and application owners. From a workflow perspective, the disparate systems and processes could affect clinical care. For instance, due to accidental oversight, a contracted physician may be given access to the EHR, but not the enterprise content management system where scanned clinical media and photos are stored. As a result, the physician's efforts to fully-understand a patient's condition and provide timely care may be delayed.

How to Effectively Address the Complexities

Identity governance is the key to enabling the organization with a single centralized view of an individual identity's access across the provider organization. It streamlines processes for determining who should have access to what and when. Identity Governance enables providers to achieve the following:

DISCOVER: Gain visibility and control of the entire spectrum of diverse data users

- Discover and determine who has access to what, when, and how access is to be granted.

SIMPLIFY: Create a simplified and consistent approach to allow for multiple and desperate authoritative sources

- Eliminate difficulties in ensuring consistent execution of security access policies.

MANAGE: Organize multiple personas of any single identity.

- Avoid critical security gaps (such as segregation of duty violations) that may occur particularly in the provisioning and deprovisioning process.

Through identity governance, providers can better cope with the complexities associated with the current healthcare IT ecosystem, and successfully scale to future requirements. To get more details about identity governance for the healthcare environment, **contact SailPoint for a free demonstration.**