WHITE PAPER

TATA CONSULTANCY SERVICES

Redefining Security Strategy in Healthcare

Abstract

The evolution of digital technologies that enabled the shift from paper-based to digital records has given rise to a new set of challenges. Different stakeholders are now collecting an exploding volume of patient, provider, payer, and hospital data. This data needs to be secured as per the prevailing norms and regulations. Furthermore, increased use of electronic personal health information (ePHI), cloud-based applications, IoT-enabled devices, and telemedicine has resulted in complex healthcare delivery networks that are prime targets for Cyberattacks. In 2018 alone, almost half (48%) of all consumer data breaches happened in the healthcare sector[1]. Given most commonly targeted data attributes in healthcare include social security numbers, health information, and financial information, the impact of such attacks is also felt more severely than in any other sector.

A new security strategy, built around strong identity and access management, can help the healthcare organizations safeguard their network and data against these evolving threats.

Reimagining the Security Perimeter

With an exponential increase in the number of connected devices, workforce decentralization, and cloud-enabled applications and systems, previously well-defined security perimeters have blurred. CIOs, CEOs, and CISOs must now secure the whole enterprise while enabling users to access sensitive data from anywhere, using multiple channels and devices. However, granting access comes with a unique set of challenges in healthcare.

The clinical staff generally comprises different types of users with varying access requirements depending on their environment, location, institution, and role. Business, IT, and other administrative users – as well as affiliates, contractors, and vendors – all require access to different applications and information. However, healthcare is one of the only industries where internal actors are the biggest threat to an organization[2]. As such, when it comes to controlled access, all the human interaction points must be considered along with non-human access, such as devices. The complexity of clinical workflows in this highly regulated ecosystem presents yet another challenge. Surrounded by an evolving need to enable intuitive user experiences and workflow efficiency, these access requirements make the security infrastructure highly vulnerable.

In this flexible, interconnected, and cloud-based reality, identity and access management (IAM) holds the key to preventing cyberattacks.

Comprehensive IAM solutions that go well-beyond single sign-on (SSO) can support not only all types of users and devices but also provide secure access to essential applications and data.

Healthcare Identity Automation Framework

IAM solutions can be implemented across different layers of a healthcare organization. Any organization that needs to implement an IAM framework can start with Identity Lifecycle and then can scale up to governance and audit compliance.

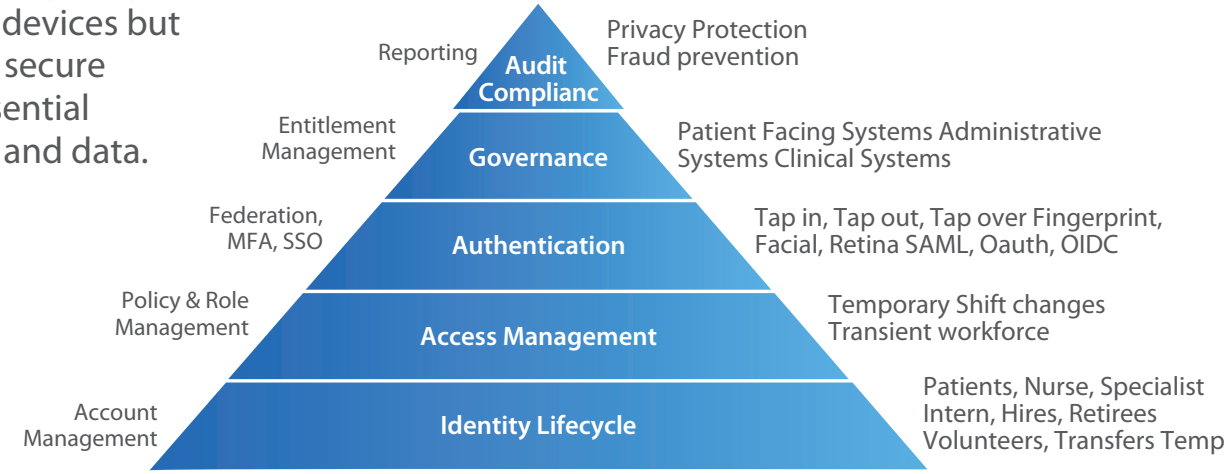

Fig 1: Identity Automation Framework for Healthcare Organizations

[1] https://www.forgerock.com/resources/view/92170441/indutry-brief/us-consumer-data-breach-report.pdf
[2] https://www.verizon.com/about/news/new-report-puts-healthcare-cybersecurity-back-under-microscope

- **Identity Lifecycle**
  Implementing IAM across this layer can help detect prolonged periods of inactivity for users like employees, visiting physicians, nurses, visitors, and patients, thereby simplifying risk assessment. Moreover, the changing ecosystem of identities such as students becoming residents, residents becoming full-time employees, departmental changes, and promotions can also be tracked. This helps ensure right individuals have access only to the data that is relevant to them.

- **Access Management**
  The way an organization applies identities to the data and resources within its environment is governed by its access management strategy. Role-based access management (RBAC) is one of the most used access management models for assigning users to groups and then applying different access to the identities in their roles. Organizations can also implement attribute-based access management (ABAC), which is based on establishing a set of attributes for various elements of the system. It establishes a central policy that defines what combinations of user and object attributes are required to perform any action. Cloud technology, SaaS, EMRs, and other applications secured with a combined model of role- and attribute-based access implementation can limit the east-west traffic for the bad identities once they get access and minimize the risks of access gained by the bad actors.

- **Authentication**
  It is a strategy used for authenticating various users across the organization and helps identity automation with federated login, multi-factor authentication, and tap-in and tap-out capabilities for simplifying access to data in clinical workflows and SaaS platforms. Smart implementation of this framework can provide access to the back-office systems along with additional factors of identity validation like time of the day and location of the request, which, in turn, can be combined to form a holistic set for eliminating cross-chatter and bad-actor activity.

- **Governance**
  A comprehensive governance strategy simplifies entitlement management and helps create a governance model across the organization. The above framework of IAM uses lifecycle management as the foundation. This simplifies the discovery of the identity lifecycle, which, in turn, provides certification of access to identities. Such a model would allow organizations to establish comprehensive governance. For instance, the Health Insurance Portability and Accountability Act (HIPAA) is generally applicable for an annual review. However, with this framework, monthly and quarterly reviews can be put in place.

- **Audit and Compliance**
  With the growing need for audit and compliance, streamlined reporting becomes critical. This layer defines the reporting strategy for the data accumulated by the IAM solution. The pyramid framework includes a reporting authentication layer with a deep-dive on how those authentication methods are being leveraged and how the reporting mandates are controlled.

Healthcare IAM Maturity Model

To get started with IAM implementation, organizations need to understand the broader IAM maturity model and then evaluate their current landscape and processes.

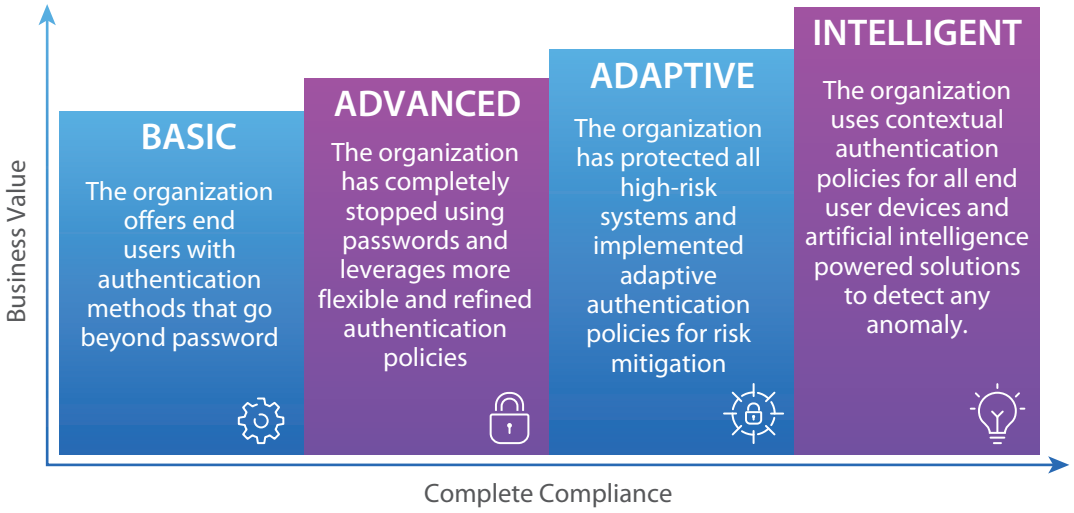

Fig 2: IAM Maturity Model

The basic model provides end-users with a basic user authentication mechanism with additional functions of tap-in and tap-out. Apart from this, it also offers lifecycle and basic access management that provides the baseline for an organization to protect its resources.

The second level of the advanced IAM maturity model augments the basic level by completely removing passwords throughout the organization and enabling multifactor authentication (MFA) or push technology. The implementation also enables role-based authorization access (RBAC) and attribute-based authorization access (ABAC).

Adaptive IAM adapts to the stringent authentication processes based on the likelihood that access to a given system could potentially result in compromising the security. It uses a scoring system where a risk score is developed for each log-in attempt, and then the score is weighed against the allowed risk threshold for a given system. Adaptive authentication

includes a software token element comprising several factors, including network information, user information, positive device identification (i.e., device forensics, user pattern analysis, and user binding), user profiling, and high-risk challenge/response questions.

MFA, if not implemented properly, can negatively impact the user experience. The intelligent IAM maturity model leverages AI to provide scenario-based MFA, which, in turn, improves user experience. It also offers other capabilities like certification compliance and segregation of duties.

Conclusion

The rising number of incidents related with healthcare data breach, and the associated costs, have put an increased focus on the need for advanced security implementation. As the use of hybrid cloud infrastructure, Internet Of Medical Things (IoMT), mobile-first experiences, and other emerging digital innovations increase, healthcare organizations will need to look beyond the traditional security means and opt for a comprehensive IAM implementation. The security framework discussed in this white paper can act as a starting point on their journey towards an evolved, resilient, and future-proof security landscape.

About The Authors

Dip Narayan Das

Dip Narayan Das is Global Head of Healthcare Technology for Tata Consultancy Services Healthcare ISU. He is an industry thought leader, strategist and partner advisor working with some of the top healthcare payer and provider organizations on operational excellence, removing cost complexity, leveraging next gen healthcare innovation, and adoption of digital technology disruption. Dip has also worked in the sphere of transformation of care management and care delivery operations to achieve value-based goals. As a cross functional IT transformation leader, he has successfully lead org transformation as part of divestiture, partner advisor for business ecosystem transformation initiatives, and organizational adoption of customer centric design experience.

Indranil Ghosh

Indranil Ghosh is Chief Architect of Technology & Transformation - Healthcare ISU. He currently leads growth and transformation initiatives in TCS' HealthCare Unit focusing on Cloud native solutions, DevOps, Intelligent Automation and Micro services architecture. He has over 20 years of experience in designing and developing complex IT solutions in the area of Web and Mobile applications, Application Programming Interface (API), Content Management Systems (CMS), Customer Relationship Management (CRM) and Digital Asset Management (DAM).

Contact

Visit the Life Sciences & Healthcare page on www.tcs.com

Email: healthcare.solutions@tcs.com

Subscribe to TCS White Papers

TCS.com RSS: http://www.tcs.com/rss_feeds/Pages/feed.aspx?f=w
Feedburner: http://feeds2.feedburner.com/tcswhitepapers

About Tata Consultancy Services Ltd (TCS)

Tata Consultancy Services is an IT services, consulting and business solutions organization that delivers real results to global business, ensuring a level of certainty no other firm can match. TCS offers a consulting-led, integrated portfolio of IT and IT-enabled infrastructure, engineering and assurance services. This is delivered through its unique Global Network Delivery Model™, recognized as the benchmark of excellence in software development. A part of the Tata Group, India's largest industrial conglomerate, TCS has a global footprint and is listed on the National Stock Exchange and Bombay Stock Exchange in India.

For more information, visit us at **www.tcs.com**

Experience certainty. IT Services
Business Solutions
Consulting

Corporate Marketing | Design Services | M | 09 | 20