

Identity and Access
Management for
Life Sciences and
Healthcare (LSHC)

Current LSHC cyber threat landscape

The LSHC industry is at the cusp of change. The main drivers for this change include:



Digital transformation

Patient experience

Clinical efficiencies

New care models

With the adoption of digital technologies, healthcare has taken a quantum leap to transform several clinical processes. On the other hand, regulatory changes, such as [guidelines for the use of telemedicine released by the government in 2020](#), have further given an impetus to healthcare organisations to modify their processes.

Today, the key factors responsible for changing the LSHC landscape include:



Adapting to changing consumer needs, demands, and expectations



Using new care delivery models to improve access and affordability



Adopting zero-trust for enhanced cybersecurity



Maintaining regulatory compliance



Investing and enhancing digital innovation and transformation

Among these key factors, maintaining regulatory compliance and enhancing cybersecurity have emerged as unique. If not addressed appropriately, they may derail the entire digital transformation programme for an organisation. As digital adoption increases, it leads to an increase in the threat surface and would lead to a situation where cybersecurity investments must be increased accordingly.

Since 2020, the attacks on LSHC organisations have been on the rise, and in some cases, the attacks have been in very specific categories, like ransomware. Hospitals, pharmaceutical companies, as well as health-tech firms have become cautious towards the impending attacks from threat vectors.

Cyber incidents can result in a loss of credentials for the organisation, as well as:

Breach of patient confidentiality

Clinical and research data loss

Regulatory impact in cases where operations have been affected due to cyber incidents

Brand and reputation loss among the patient and healthcare community

Cybersecurity challenges in healthcare

Healthcare organisations contain confidential patient information, including diagnostic plans, medical history, reports, and prescriptions that can be misused by threat actors. Not only do these records fetch lucrative offers on the dark web, but also be used to create fake identities and commit other fraudulent activities. Reputation loss, disruptions in operations, as well as loss of revenues from areas like medical tourism also affect the revenues of healthcare organisations. Hospitals use sophisticated healthcare applications and devices, and administrative access to these, if compromised, can cause a greater risk of cyberattacks.



Protected Health Information (PHI) is 50 times more valuable in the black market than financial information. Stolen patient health records are sold at value 10-20 times more than credit card information.



Identity & Access Management (IAM) – Solution for the LSHC cybersecurity needs

There is a need to adopt an agile and dynamic security foundation that is resilient to organisational change and flexible enough to meet the challenges faced by the modern business, workforce, and technology trends. A zero-trust security model helps establish this security foundation and reduce cyber and data risks and managing digital identities (human and non-human). A robust IAM solution helps safeguard sensitive clinical and personal health records, and business critical infrastructure from unauthorised access. It also shields your organisation from security threats. An IAM framework also automates lifecycle management processes for the workforce and devices in healthcare organisations, improves operational efficiency, and reduces help desk calls and costs. Whether your organisation keeps its data in the cloud, on-premise, or in a hybrid environment, an IAM solution seamlessly helps you to operate securely in a connected world.

Here is a glimpse of typical IAM use-cases in a healthcare organisation:



Identity Governance and Administration

- Patient registration and self-service on healthcare portals
- Contractor, vendor, and supplier access management
- Role optimisation, segregation of duties, role-based access rights control for sites, studies, labs, etc.
- Access reviews, auditing, reporting, risk monitoring and detection using analytics

Access Management

- Omni-channel experience to cater to the surge of digital touchpoints
- Connect sites in different geographies and streamline the healthcare process using federated single sign-on
- Device registration & fingerprinting
- Enable single sign-on to enhance user experience while preventing cyberattacks by malicious actors
- Enable multi-factor authentication for access to highly sensitive healthcare applications and transactions

Privileged Access Management

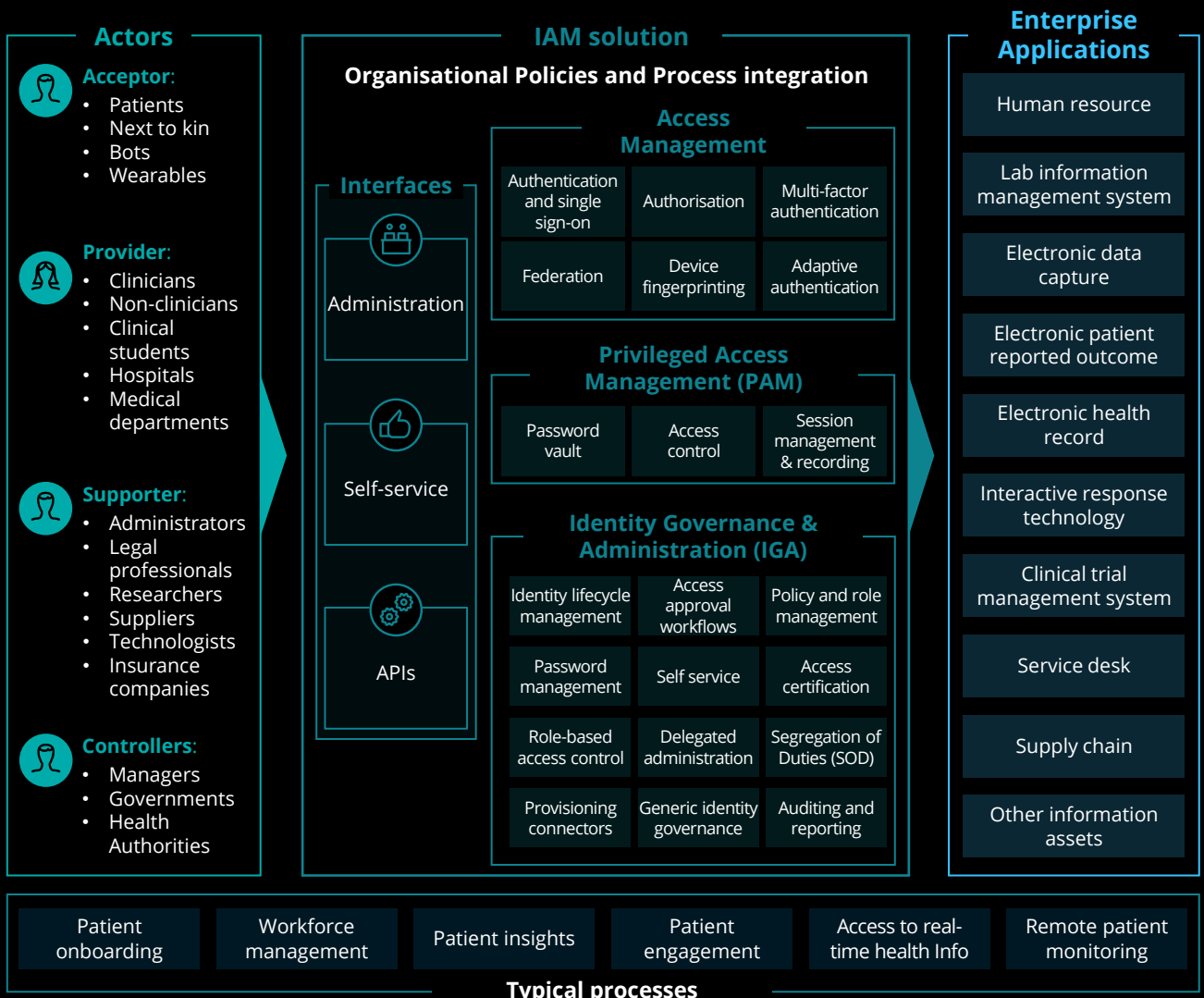
- Comprehensive monitoring, recording and isolation of all privileged user sessions, detailed activity reports on critical ePHI database or applications
- Automated, end-to-end detection and protection for all privileged access
- Privileged threat detection and analytics to respond and remediate to any anomalous or high-risk activities

Solution overview

The IAM solution acts as a centralised and shared service to manage and administer the digital identities and their access to the critical IT resources based on the least access principle.


- The Identity Governance and Administration (IGA) component of the solution can manage the user/device identity lifecycle and automate the entire user lifecycle (both internal and external) for organisations. It can support them to access provisioning and deprovisioning to the integrated enterprise applications and platforms.
- The Access Management component of the solution allows secure user access to protected applications. It enables capabilities, including friction-less and risk-based authentication using biometrics and mobile devices, least privilege using risk-based authorisation, and Single Sign-On (SSO) for enhanced user experience.
- The Privileged Access Management (PAM) component of the solution can help organisations manage and monitor the privileged user access, including system/network/database administrators, service accounts, and generic accounts, for the underlying operating system platforms, network devices, databases, and cloud platforms.

These components can also help organisations generate reports that can be used to address compliance requirements.



Key benefits

LSHC organisations should consider IAM as an integral part of their cybersecurity strategy. It is instrumental in responding to new business challenges, in addition to providing core benefits as follows:



Regulatory compliance

Compliance with regulations related to patient privacy, including, but not limited to, Health Insurance Portability and Accountability Act of 1996 (HIPAA). Some IAM products also offer built-in HIPAA compliance and reporting.

Operational efficiency

Automated key identity management processes reduce maintenance and support costs, and decrease turnaround time for user onboarding, offboarding, password management, and access-request processing.

Enhanced security posture

Enhanced authentication can fortify and monitor web applications, cloud servers, and patient portals in which healthcare systems operate. Single source of truth, well-defined access policies, and governance checks help enhance the enterprise security posture.

Improved user experience

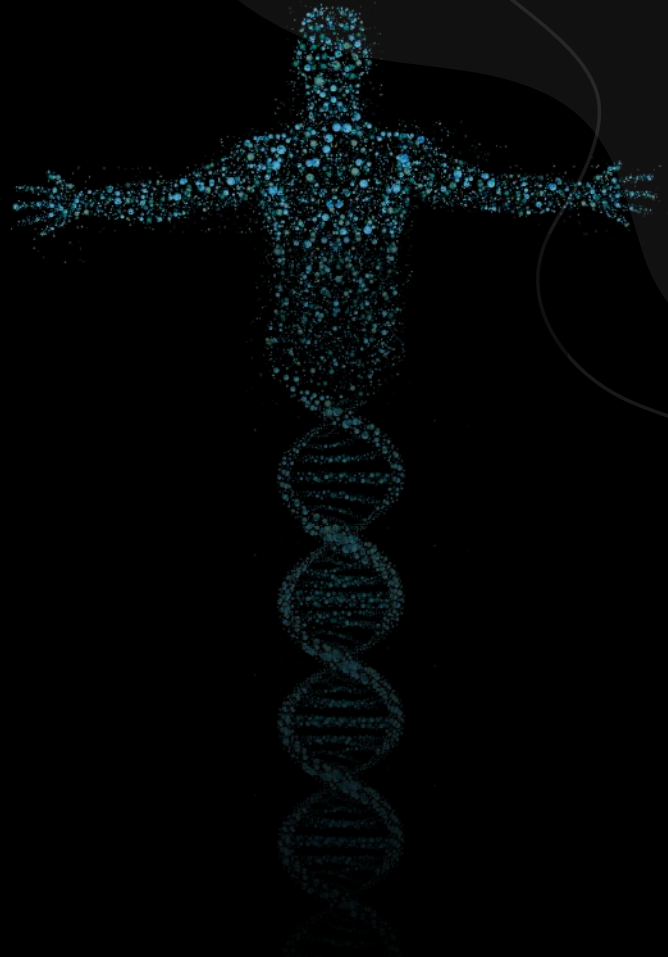
Increased visibility into the access request process, seamless SSO experience to multiple portals, single login credentials, and one digital identity that unlocks the door to many services.

Reduced IT complexity

Use of standards-based integration capable of spanning both legacy and modern technology, ability to scale to millions of users, and providing capabilities that allow healthcare portals to integrate with the cloud and on-premises services.

The future of health

According to Deloitte's future of cyber in the future of health report - "In the future of health, nearly everything will be connected through digital technologies to meet the common goal of improving patient well-being and care. And cyber will be integral to each of these exciting advancements." With enormous amounts of patient data being gathered and shared every second, it will be imperative to secure access to patient's information and prevent it from emerging risks and threats. In the age of the Internet of Healthcare things (IoHT), not just patient data but also use of healthcare devices and wearables is expected to witness growth. A Gartner report on Wearable Electronic Devices, Worldwide (2019) forecasts that "By 2023, device makers will focus on offering smaller, clinical-grade sensors for health wearables that increase monitoring accuracy by 20%." Trusting these devices, and moreover the data they generate, would be a riveting challenge for healthcare organisations to solve. In addition to this, consumer devices would also need to be registered and linked to consumers. Healthcare organisations must put in a deep thought and strategise on a sound identity and access management roadmap, to be able to combat these challenges as this domain advances.



Contact us

Anthony Crasto

President, Risk Advisory
Deloitte India
acrasto@deloitte.com

Abhijit Katkar

Partner, Risk Advisory
Deloitte India
akatkar@deloitte.com

Kamaljit Chawla

Leader – Cyber Operate
Risk Advisory, Deloitte India
kamaljitc@deloitte.com

Tarun Kaura

Leader – Cyber Advisory
Risk Advisory, Deloitte India
tkaura@deloitte.com





Vikram Venkateswaran

Partner, Risk Advisory
Deloitte India
vikramv@deloitte.com

Ravindra Usmanpurkar

Director, Risk Advisory
Deloitte India
uravindra@deloitte.com

Sources

-  [The future of cyber in the future of health \(Web\)](#)
-  [The future of cyber in the future of health \(PDF\)](#)
-  [Health care cybersecurity](#)
-  [Gartner Forecast Analysis: Wearable Electronic Devices, Worldwide](#)

Black Book State of the Healthcare Industry Cybersecurity Industry Report:

-  [State of the Healthcare Cybersecurity Industry](#)
-  [Data Exposure is a Communicable Disease](#)
-  [The Future of Identity Management](#)
-  [Authentication and Identity Management of IoHT Devices: Achievements, Challenges, and Future Directions](#)
-  [What to Expect: Future Trends in Identity and Access Management](#)

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee (“DTTL”), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as “Deloitte Global”) does not provide services to clients. Please see www.deloitte.com/about for a more detailed description of DTTL and its member firms.

This material is prepared by Deloitte Touche Tohmatsu India LLP (DTTILLP). This material (including any information contained in it) is intended to provide general information on a particular subject(s) and is not an exhaustive treatment of such subject(s) or a substitute to obtaining professional services or advice. This material may contain information sourced from publicly available information or other third party sources. DTTILLP does not independently verify any such sources and is not responsible for any loss whatsoever caused due to reliance placed on information sourced from such sources. None of DTTILLP, Deloitte Touche Tohmatsu Limited, its member firms, or their related entities (collectively, the “Deloitte Network”) is, by means of this material, rendering any kind of investment, legal or other professional advice or services. You should seek specific advice of the relevant professional(s) for these kind of services. This material or information is not intended to be relied upon as the sole basis for any decision which may affect you or your business. Before making any decision or taking any action that might affect your personal finances or business, you should consult a qualified professional adviser.

No entity in the Deloitte Network shall be responsible for any loss whatsoever sustained by any person or entity by reason of access to, use of or reliance on, this material. By using this material or any information contained in it, the user accepts this entire notice and terms of use.