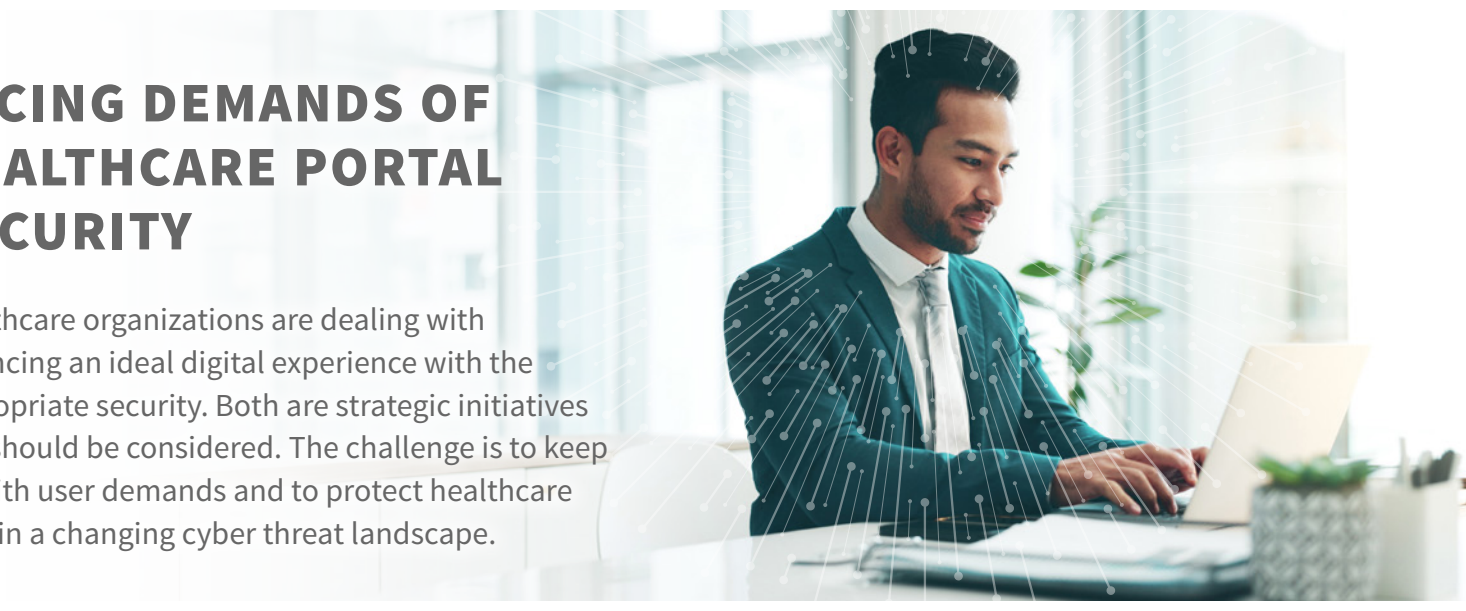
LexisNexis® RISK SOLUTIONS | Healthcare

FACING DEMANDS OF HEALTHCARE PORTAL SECURITY



Healthcare organizations are dealing with balancing an ideal digital experience with the appropriate security. Both are strategic initiatives and should be considered. The challenge is to keep up with user demands and to protect healthcare data in a changing cyber threat landscape.

Meeting the Challenges of Protecting Healthcare Portals

Healthcare portals are essential for patient and member engagement, but many are vulnerable and under-optimized. As digital engagement becomes the norm, poorly designed portals can frustrate users, erode trust, increase costs and expose sensitive data. To address these challenges, organizations need secure, user-friendly digital experiences that protect patient information and foster engagement. This section outlines key risks and opportunities for strengthening portals in today's digital-first healthcare landscape.

In 2024, The OCR (Office for Civil Rights) reported **720 incidents, impacting 186 million people**[1]

A single phone interaction can cost **up to 80 times more** than a digital engagement[2]

88% of users won't return to a website after a poor experience[3]

Building a Business Case to Align on Strategy and Value

It's important to align the organization on critical parameters, determine cost and revenue impact, and build a business case. As you build your case, you will discover aspects that may have been overlooked or existing processes that have been working. A business case is a transparent, collaborative way to successfully align on a strategic path that considers risk, user experience and value. Don't think of this process as a business case to justify investments for a point in time. Think of it as a roadmap for how your business will operate into the future.

Determine risk tolerance across digital transactions to determine what types of security solutions you need.

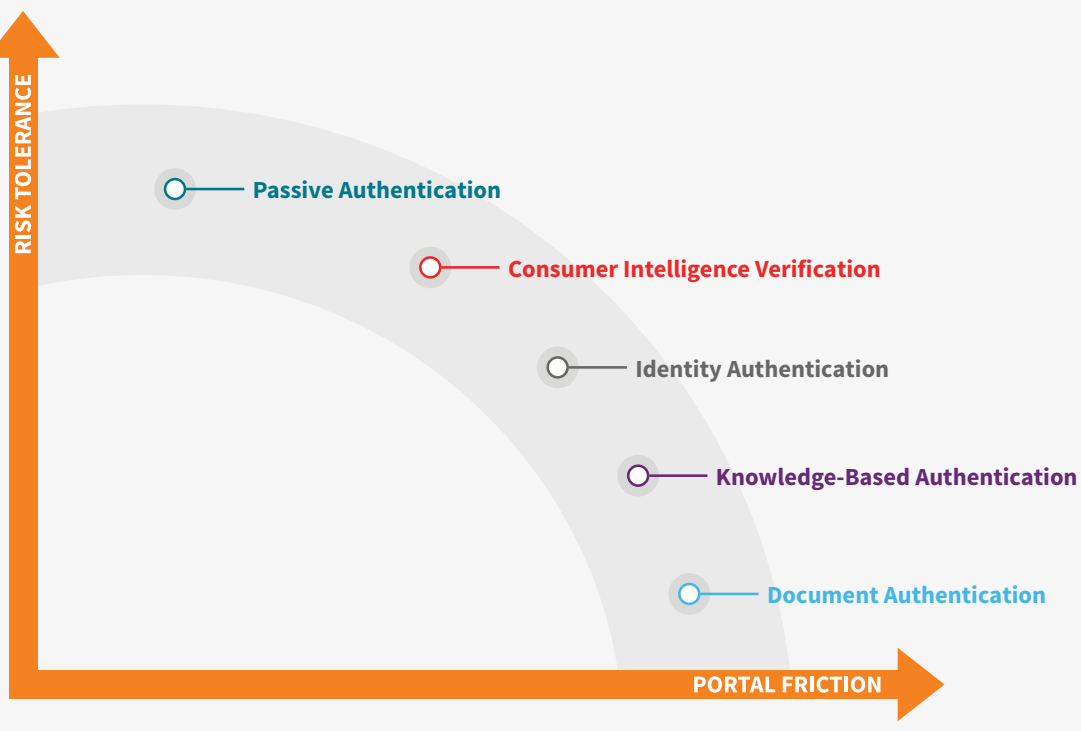
Align stakeholders on goals and metrics to measure success.

Calculate ROI by looking at costs, cost savings and revenue impact. Use ROI to determine the value of a potential solution investment.

How to Balance Security and Digital Experience by Combining Advanced Solutions

To address the challenge of finding the right balance of security and digital experience, you need to consider your risk tolerance levels and patient/member satisfaction. Find an identity verification solution partner that can give you access to a full spectrum of solutions from passive capabilities like digital identity verification to more secure multi-factor authentication. You can combine solutions to meet your specific organization's needs.

Create your **ideal balance of risk tolerance and digital experience.**



If you think you have to sacrifice a positive digital experience to meet organizational risk tolerance, let us help you explore solutions that enable you to achieve both.

CONTACT US

References

1. 2024 US Healthcare Data Breaches: 720 Incidents, 186 Million Compromised User Records, https://www.securityweek.com/2024-us-healthcare-data-breaches-585-incidents-180-million-compromised-user-records/
2. Gartner Says Only 9% of Customers Report Solving Their Issues Completely via Self-Service, https://www.gartner.com/smarterwithgartner/rethink-customer-service-strategy-drive-self-service
3. op Website Statistics Today, https://www.forbes.com/advisor/business/software/website-statistics/