

**Building an Effective
Healthcare Digital
Experience Business Case**



Healthcare organizations have come to understand that the post-COVID consumers are demanding positive digital experiences. Consumers want an easy, fast online experience. Too few security measures, and you leave yourself open to debilitating and costly cyberattacks. Too many, and you frustrate your consumers with an onerous online experience. Organizations need to find the balance between the two.

One approach is to focus on key experiences that are the initial entry to your digital front door from initial entry to repeated logins. A bad front door experience will result in new account registration failures and failure of individuals to return for subsequent logins. An estimated 88% of consumers who have a bad experience won't return to a website.¹ Prioritizing digital experience can benefit your organization. In many cases, a successful online interface and effective digital tools drive down administrative costs, handle many routine tasks that free up physician, pharmacist and staff time, and boost consumer engagement and satisfaction. Consumers can form long-lasting impressions and remain loyal to your organization based on their digital experience.



An estimated **88% of consumers who have a bad experience won't return to a website**

Traditional phone calls to staff can cost your business up to 80 times more than digital engagements.² The strategy is not to disconnect phone calls altogether, but to minimize staff time devoted to making and changing appointments, requesting medication refills, and performing other routine tasks many consumers can take care of, and often prefer to handle, online.



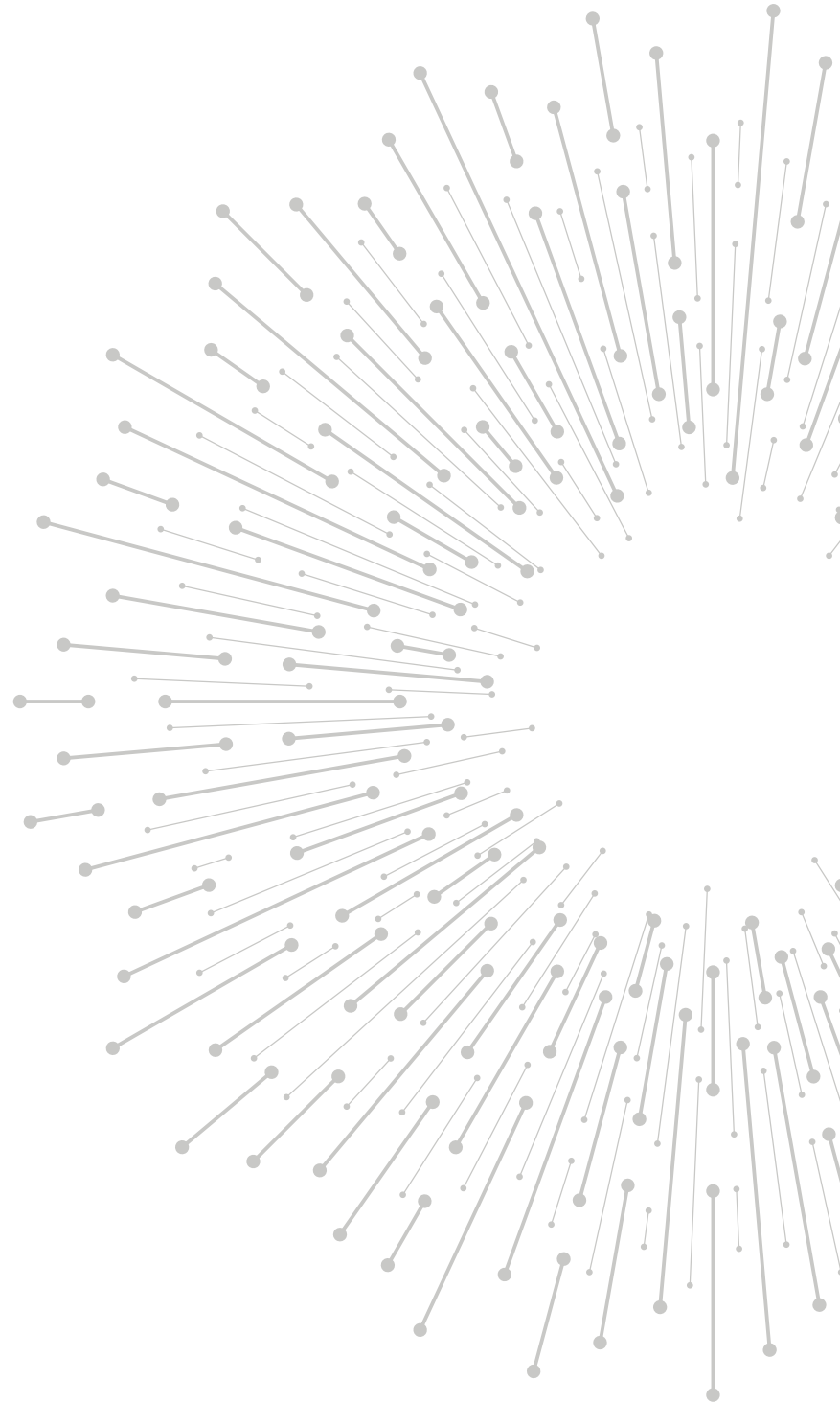
Traditional phone calls to staff can **cost your business up to 80 times more** than digital engagements

The number of breached healthcare records has increased greatly. Data from the U.S. Department of Health and Human Services Office for Civil Rights indicates a continued increase in breaches, but the number of breached healthcare records in 2023 “smashed all previous records with an astonishing 133 million records exposed, stolen, or otherwise impermissibly disclosed.”³ Portal hacking is a common threat, accounting for an estimated 1 in 5 attacks outlined in the LexisNexis® True Cost of Fraud Report™.⁴

It’s critical to invest in technology and tools that provide the right balance of lower consumer friction and higher security. Today’s solutions offer a near-frictionless consumer experience and deliver the security you need. Before you can get leadership onboard, you need a recommended solution and a business case to prove out your costs/benefits.



5 Steps to Build Your Business Case



1. Identify your organization's security policies and risk tolerance

Research your information protection and information security policies for requirements that apply to consumer-facing portals. You need to understand requirements of how your organization handles identity verification and access management. What is the risk tolerance for different types of transactions like a new account opening or a login transaction, or a high value transaction like a credit card number change or password change?

Your risk tolerance refers to your organization's willingness to accept risk levels for each of those transactions coming in. Tolerance levels can be set, and then using risk-level quantification, you can measure and react differently to different threat levels.

For example, interacting with known customers through a verified business relationship can be low risk. In contrast, login attempts from regions around the world associated with cyberattacks or known bad actors are inherently high risk. Once risk is determined, you can deploy appropriate security measures.

Your business is unlike any other, so it's likely you also have some unique risk factors. Know your more vulnerable spots and plan to prevent security breaches.



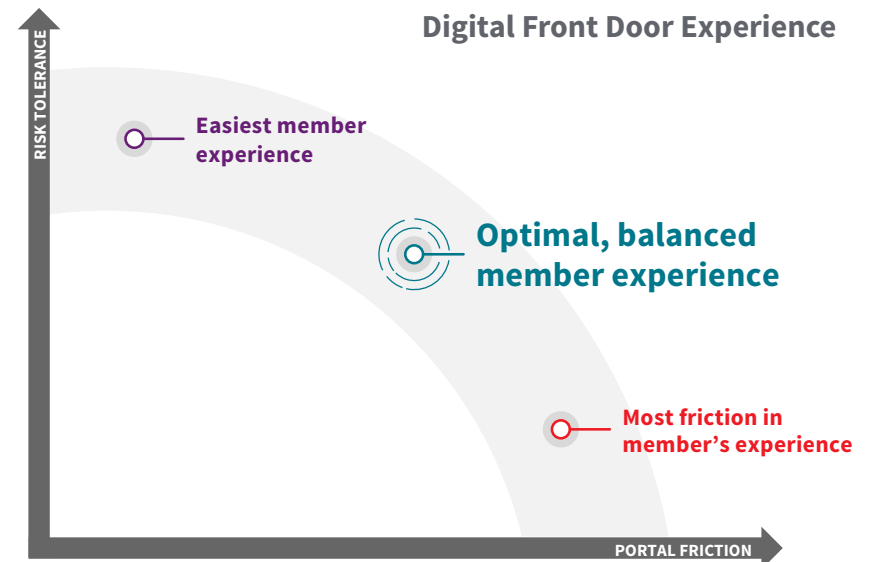
2. Define Your Consumer Digital Experience

Your digital experience is a key part of your overall consumer experience. There are several steps to striking the right balance between a positive, easy digital experience (UX) and robust online security. After determining the risk tolerance, think about the tradeoffs from a consumer perspective.

To find the sweet spot, talk to your company's customer service, process improvement and other relevant internal teams. Ask them to define your organization's digital experience and related goals which may include increasing the number of consumers on the site, moving more customer interactions online, or extending customer life value.

Think about asking questions like: Are there roles for artificial intelligence and/or chat bots now or in the near future? Where do these teams see the opportunities for improving digital experience?

Externally, evaluate consumer feedback. Check your online reviews and look for patterns that can illuminate areas needing improvement.



3. Identify Metrics that Matter, Align with Stakeholders

Whether your metrics include cost savings on administrative tasks, increased consumer use of your portal, or greater uptake of health management tools, it's important to know how you're doing on an ongoing basis.

There is strength in numbers. Consider what digital experience success looks like across your organization. Ask different stakeholders such as your operations teams, clinical outreach and care coordination teams, IT and security teams. The more stakeholders you engage, the stronger your business case for change.



Consider these types of measures to help monitor success of your investment:



Administrative cost reduction by moving phone calls to other channels



Increased utilization of your portal, such as percentage of consumers who login to your portal each month



Improved consumer engagement, such as use of digital tools on your portal



Improved consumer satisfaction survey results (like Net Promoter Score or Consumer Assessment of healthcare Providers and Systems (CAHPS) surveys)

4. Estimate your cost/benefits of improved digital engagement and improved security

There are multiple types of benefits you can use in your business case to begin to justify the investment in digital experience and security. As you explore the priorities of your security team and consumer-facing teams, here are some of the categories of benefits to consider in your business case:

Cyberattacks and data breaches cost more than prevention.

A data breach can cost millions of dollars to clean up. Healthcare data breaches cost an average of \$9.3M per incident and \$408 per stolen record.⁵ The costs of remediation, escalation and prevention all contribute.

The average cost for initial remediation and escalation is \$1.67M. Every \$1 spent on initial remediation and escalation ultimately costs payers 3.23 times that amount given additional costs of restitution, lost productivity and membership, fines, fees and mitigation investment.⁶

Additionally, the cost of cybersecurity insurance is increasing, and the stability of the market is declining, with insurers tightening the terms of policies and limiting their exposure.⁷

Replacing lost customers is costly

When you think of customer retention, you must consider the value of a lost customer which includes both marketing costs and the customer life value. It's generally accepted that acquiring a customer costs more than retaining one. Customers leave for many reasons, including data breaches which are costly:

- Data breaches often lead to loss of customers and/or trouble retaining new customers. In one report, about 55% of payers report they lost customers after a breach and 40% experienced lower new member enrollment following a breach.⁶
- Payers surveyed reported that the cost of acquiring new customers is 3 times the cost of keeping existing ones. Acquiring a new customer costs approximately \$615.⁶

Improve online utilization rates, leading to reduction in administrative costs

Good digital experience will increase utilization rates, and more people on your portal means fewer calls into your customer support, saving on administrative costs.

- When individuals were offered access to their healthcare portal, nearly 40% accessed it.⁸
- The cost of a live chat or phone call is 80x more expensive than mobile app or website costs.⁹ Some types of live customer service may be better serviced online such as medication refills or appointment scheduling.

One way to improve utilization rates and consumer engagement is to replace antiquated, one-size-fits-all security measures with risk-based security methods that support your customer experience goals and security requirements.

Improving health outcomes through online health management tools

A majority of physicians encourage customers to access and use an online portal to manage their wellbeing. Many customers are interested in managing their health using online tools such as a healthcare portal, apps integrated into a healthcare portal or even text messages. A majority of customers access portals, for the ability to communicate directly with their healthcare provider.¹⁰

Customers can schedule appointments, easily communicate with the provider office and get relevant messages for their health. Payers make information available on relevant topics like diet, reminders about health screenings, preventive measures and conditions the customer may have.

Having a digital experience that is secure and easy to use will make it easy for your customers to engage with digital tools and feel safe while doing so. More engagement leads to better health outcomes which benefits your customers' health and helps reduce operating and medical costs.

Research identity verification and authentication tools that help you reach your goals

After determining risk tolerance and the vision of your consumer experience, you need to find solutions that can help you deliver the balance between the digital experience and security.

Today, you can get solutions that are verifying consumers without them realizing it. This passive type of solution looks at digital attributes like device ID, IP address, behavioral biometrics and other digital identity factors. You can give trusted consumers a smooth easy digital experience and stop bad actors when they attempt to come through your digital front door. A range of solutions for verification and authentication are available to accommodate your defined risk tolerance.

Preventive digital security measures can cost as little as pennies per consumer per year and help you avoid any potential reputational damage or permanent loss of consumers.*

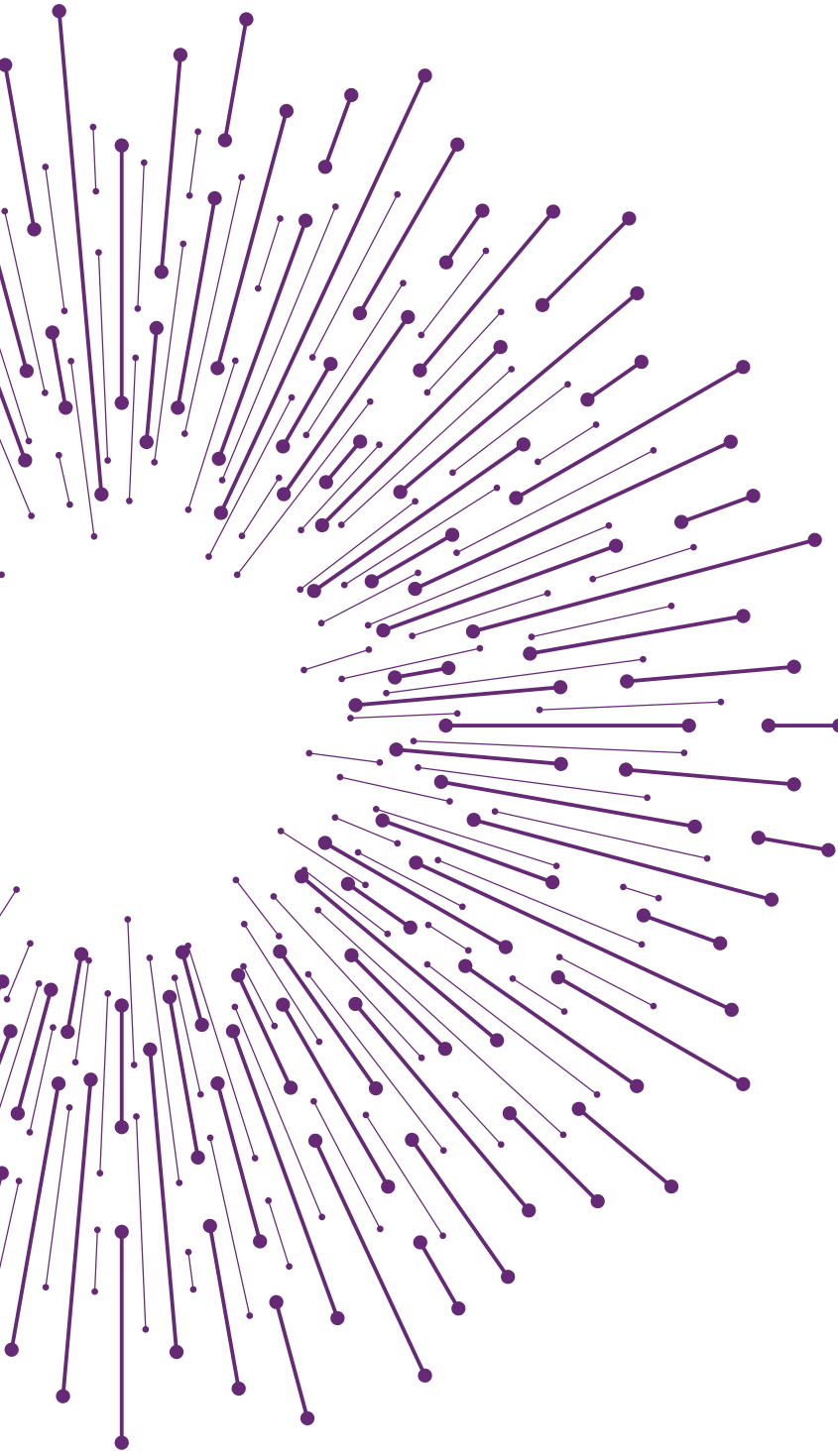
*Costs are estimated and generalized based on average costs across LexisNexis Risk Solutions shelf rates at a per consumer level.



A range of solutions for verification and authentication are available to accommodate your defined risk tolerance



Preventive digital security measures can cost as little as pennies per consumer per year



5. Start with Some Wins

An effective way to begin building your digital experience business case is to focus on a few key areas where you can make a significant impact early. You can build on those small wins over time, and strengthen your arguments for improvements in adoption, health outcome improvements and administrative cost reductions.

Need guidance to get started and keep the momentum going? Consider working with vendors that can support the often-conflicting needs of your security and customer service teams, help you select a key customer experience to start, and present your wins to your business executives.

Improving your digital experience can reap multiple benefits for your organization. Customer experience and security do not have to be in conflict. Data solutions can help you support experience goals across your organization, while delivering the security demanded by your information protection policies. A strong business case is essential for moving the needle forward on consumer experience.



Focus on a few key areas where you can make a significant impact early.



To learn more about identity verification solutions that can support your digital experience and security goals, [contact us](#).

References

- 1 [Top Website Statistics for 2023 – Forbes Advisor](#) 7 Eye-Opening Website Statistics [Updated for 2023] (sweor.com)
- 2 [Gartner Says Only 9% of Customers Report Solving Their Issues Completely via Self-Service](#)
- 3 <https://www.hipaajournal.com/healthcare-data-breach-statistics/>
- 4 <https://risk.lexisnexis.com/insights-resources/research/us-ca-true-cost-of-fraud-study>
- 5 <https://techjury.net/blog/healthcare-data-breaches-statistics/>
- 6 <https://risk.lexisnexis.com/insights-resources/research/us-ca-true-cost-of-fraud-study>
- 7 [Rising Cyberthreats Increase Cyber Insurance Premiums While Reducing Availability | U.S. GAO](#)
- 8 [Individuals' Access and Use of Patient Portals and Smartphone Health Apps, 2020 | HealthIT.gov](#)
- 9 [Gartner Says Only 9% of Customers Report Solving Their Issues Completely via Self-Service](#)
- 10 [Access and Use of Patient Portals and Smartphone Health Apps, 2020 | HealthIT.gov](#)

About LexisNexis® Risk Solutions

LexisNexis® Risk Solutions includes seven brands that span multiple industries and sectors. We harness the power of data, sophisticated analytics platforms, and technology solutions to provide insights that help businesses and governmental entities reduce risk and improve decisions to benefit people around the globe. Headquartered in metro Atlanta, Georgia, we have offices throughout the world and are part of RELX (LSE: REL/NYSE: RELX), a global provider of information-based analytics and decision tools for professional and business customers. For more information, please visit www.risk.lexisnexis.com/corporate and www.relx.com.

LexisNexis and the Knowledge Burst logo are registered trademarks of RELX Inc. Other products or services may be trademarks or registered trademarks of their respective companies. Copyright © 2024 LexisNexis Risk Solutions. NXR16325-00-0224-EN-US