Healthcare Data: A Prime Target for Cybercriminals

After years of skyrocketing digital attacks across industries, data from the annual LexisNexis® Risk Solutions Cybercrime Report shows that global cybercrime attack rates began stabilizing in 2024, with daily attacks rising by just 1%.[1] However, cyberattacks are still multiplying worldwide and remain at historically high levels. And this stabilization may be temporary as cybercriminals retool their approaches with increasingly sophisticated methods, including generative AI-powered attacks.

Although hackers don't discriminate, healthcare remains a prime target for cybercrime, given the amount of confidential data stored within its systems and less robust identity verification methods. A flexible, multi-layered fraud prevention strategy has never been more critical.

GLOBAL CYBERSECURITY TRENDS

LexisNexis® Risk Solutions analyzed more than 100 billion transactions across industries in 2024. The analysis found that bot attacks shrank while human-initiated attacks grew. For healthcare organizations, this underscores the need for adaptive, user-centric security strategies that account for evolving means of attack and the growing use mobile devices in patient engagement.

U.S. Region

YoY Human-Initiated Attacks in the U.S **Up 24%** to 511 Million Occurrences

Overall Attack Rate in U.S. **Higher** Than Overall Global Attack Rate (1.7% vs. 1.5%)

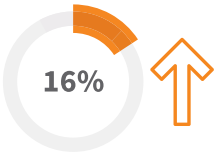
U.S. Attack Rates on **Mobile** More Than 1.5x Higher Than Desktop (62% vs. 38%)

Global

1 in Every 11 New Account Creations are Attacks

YoY Human-Initiated Attacks

16% increase in volume of high-risk fraud attacks



Human-Initiated Attack Volume		Human-Initiated Attack Rate		YoY
73%	Mobile	Overall:	1.5%	+1%
27%	Desktop	Desktop:	2.1%	+6%
		Mobile Browser:	3.9%	+4%
		Mobile app:	0.8%	-6%

RISK TRENDS

Attack rates on high-value actions, like changes to account details, are rising sharply, with a 92% YoY increase. These trends highlight how cybercriminals are increasingly targeting points of vulnerability that may provide broad access to sensitive healthcare information.

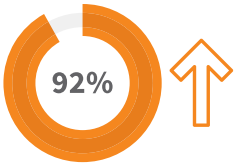
Password Resets

Overall Attack Rate Percentage:	11.1%
Desktop Attack Rate Percentage:	27%
Mobile Browser Attack Rate Percentage:	2.3%
Mobile App Attack Rate Percentage:	0.7%

Change in Account Details

Interception of authentication messages such as one-time passcodes occur by changing the account's registered phone number or email address.

YoY Increase in Attacks Involving a Change of Account Details



User Account Detail Changes

Overall:	7.3%
Desktop:	12.6%
Mobile Browser:	15.1%
Mobile app:	1.4%

Attack volume and attack rate by use case are calculated using a subset of the total transaction volume, where outliers and unknown sessions are removed.

Healthcare Consumers Expect Convenience and Security

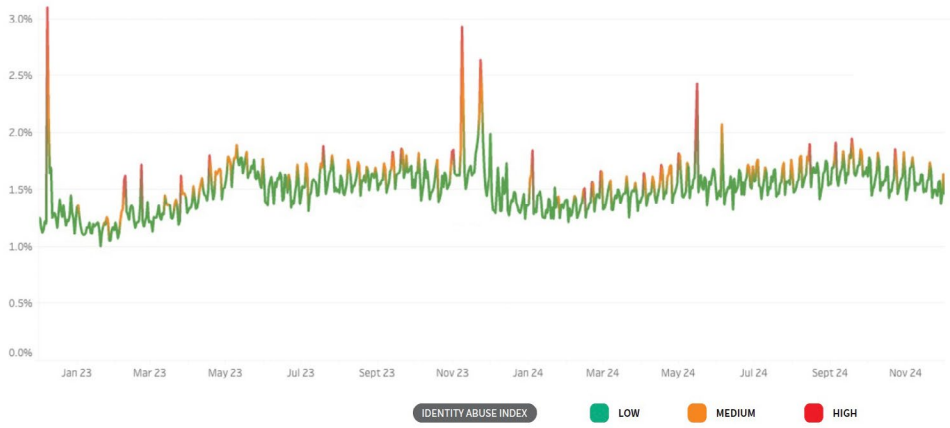
Today, consumers expect their healthcare experiences to be similar to those of other industries: fast, convenient and online. They want healthcare to be as easy as booking a flight or shopping online. With roughly 60% of individuals being offered and accessing their online medical record or patient portal, they also demand secure interactions that protect their personal health data.[2]

Growing consumer ownership of medical records, digital portal expansion, interoperability and other trends require healthcare organizations to effectively protect patient data from exposure to fraud.

While other industries like banking and ecommerce have modernized their consumer digital interactions, many healthcare organizations still rely on legacy identity verification methods, often prioritizing ease of access over robust security. These vulnerabilities across touchpoints, including logins, payments and new account creations, make healthcare organizations an easy target for cybercriminals.

LEXISNEXIS® IDENTITY ABUSE INDEX

The LexisNexis® Identity Abuse Index shows the percentage of attacks per day across the entire LexisNexis® Digital Identity Network® platform, including both human-initiated and sophisticated bot attacks. Analyzing more than 100B transactions across multiple industries, this index was relatively calm this year, showing little sustained growth YoY (1%), as popular concerns about increased threats linked to AI have so far proved unfounded. However, cybercriminals' initial focus may have been on testing these new technical capabilities with smaller attacks, possibly driving up AI attack rates in next year's data.



Peaks may occur during periods of high transaction rates, such as Black Friday in ecommerce, holiday season for the food and beverage industry or open enrollment and new account set up in the healthcare industry.

"Since most successful attacks are performed using leaked user credentials, strong multi-factor authentication is a must. The key is balancing a rigorous authentication process with a convenient user experience."

- FLAVIO VILLANUSTRE
Chief Information Security Officer, LexisNexis® Risk Solutions

HEALTHCARE DATA SECURITY TRENDS

1.74% The number of large healthcare data breaches dropped slightly in 2024.[3]

64.1% However, the number of records breached was much greater.[4]

+81% of the U.S. population was impacted by a breach.[4]

$9.77M Average cost of a healthcare data breach.[5]

70% Breached healthcare organizations that reported significant or very significant disruption.[4]

63% Healthcare organizations that passed on breach-related costs to consumers.[4]

LexisNexis® RISK SOLUTIONS | Healthcare

AI's Growing Role in Cyberattacks

Although global attack rates began stabilizing in 2024 after two years of substantial increases, they remain at historically high levels. To date, the use of generative AI to grow and scale attacks has been limited. However, cybercriminals' initial focus may have been on testing these new technical capabilities with smaller attacks, and we may see AI drive attack rates in the coming years. In fact, in a survey of 650 cybersecurity experts, 85% attributed recent rises in cyberattacks to criminals using generative AI.[6]

Building a Strong Defense Against Digital Attacks

Detecting online attacks requires healthcare organizations to take a comprehensive, multi-layered approach. A defense against cybercriminals should bring together data, generative AI, predictive analytics and a strong understanding of the evolving cybersecurity threat landscape. The most successful approaches involve:

- ☑ Evaluating device identifiers and IP addresses to assess risk and identify suspicious activity before it becomes a problem
- ☑ Comparing user behavior to historical patterns to identify anomalies, allowing only legitimate users to gain access
- ☑ Placing users flagged as higher risk into a customized authentication workflow, like one-time passwords
- ☑ Enforcing strong multi-factor authentication
- ☑ Robust encryption and mature key management processes to protect sensitive data both in transit and at rest

BALANCING PORTAL SECURITY WITH DIGITAL EXPERIENCE

High-profile breaches targeting major healthcare organizations in 2024 reinforced the vulnerability of healthcare data and the need to protect against breaches while giving consumers a seamless, convenient experience.

Your strategy for securing your healthcare portals from unauthorized access should evolve with today's risks. Organizations with sophisticated defenses and AI-optimized detection policies are successfully securing their environments against rising threat levels. Learn how to mitigate identity verification risks while delivering an exceptional digital experience for patients and members.

Visit risk.lexisnexis.com/healthcare/identity-verification to learn more.

1 LexisNexis Risk Solutions 2024 Global Cybercrime Report
2 https://www.healthit.gov/data/data-briefs/individuals-access-and-use-patient-portals-and-smartphone-health-apps-2022
3 https://www.hipaajournal.com/healthcare-data-breach-statistics/
4 https://www.hipaajournal.com/biggest-healthcare-data-breaches-2024/
5 https://www.hipaajournal.com/cost-healthcare-data-breach-2024/
6 https://www.forbes.com/sites/jeffkauflin/2023/09/18/how-ai-is-supercharging-financial-fraudand-making-it-harder-to-spot/?sh=1ca05fcd6073

LexisNexis® RISK SOLUTIONS | Healthcare