LexisNexis® RISK SOLUTIONS | Health Care

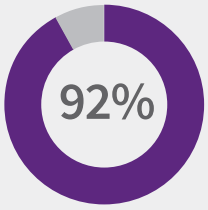
LexisNexis® Device Assessment for Providers

Frictionless, real-time authentication to better protect patient data

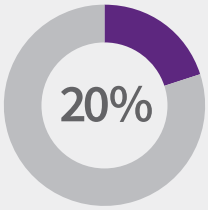
The healthcare industry continues to move towards digitization with the increased use of mobile devices (i.e. cellular devices, tablets, laptops, etc.) to access health information. The use of online portals has created expansive security vulnerabilities and attracted an increased volume and variety of cyber fraud. The need to maximize security while maintaining a positive patient experience has fueled the evolution of a multi-layered approach to the onboarding and authentication of new patients. LexisNexis® Device Assessment offers an ideal first layer of defense.

LexisNexis® Device Assessment for Providers

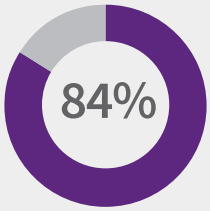
Healthcare has gone mobile



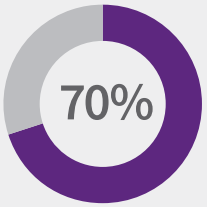
OF PATIENTS CAN ACCESS HEALTH RECORDS DIGITALLY VERSUS 43% JUST TWO YEARS PRIOR[1]



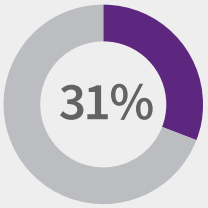
HIGHER RETENTION RATES FOR NEW PATIENTS THAT SIGN UP FOR A PORTAL ACCOUNT WITHIN 30 DAYS OF THEIR VISIT[2]



OF SURVEYED CARE PROVIDERS ARE USING MOBILE DEVICES; PRIMARILY TABLETS; FOR POST-HOSPITAL DISCHARGE SUPPORT[3]



OF SURVEYED DOCTORS USE MOBILE DEVICES TO MANAGE IN-PATIENT DATA[4]



OF PATIENTS HAVE USED A MOBILE APP TO COMMUNICATE WITH THEIR HEALTHCARE PROVIDER[5]

Mobile has created a feeding frenzy of fraudulent activity:

- BOT activity is in an uptrend, after a three-year decline[6]
- Medical identity theft and big data breaches in the medical industry have been on the rise[7]
- Data breaches have made identities commodities for cyber criminals

1 American Hospital Association; 2 Athena Health; 3 Fierce Mobile Healthcare IT; 4 Black Book Market Research; 5 West Monroe Partners; 6 Incapsula; 7 Consumer Reports/Ponemon Institute

Security and patient friction are a balancing act

The pressure of more mobile activity and more security risks has created additional challenges:

- Patients are demanding better security and privacy
- Frequent and obtrusive step-up challenges frustrate patients
- Cyber criminals are sharing data across growing fraud rings
- Traditional, static authentication methods are no match for sophisticated fraudsters
- Costs of fraud encompass patient attrition, fines, reputational damage and lost profits

LexisNexis Health Care has reinvented authentication

LexisNexis leverages its decades of experience in identity authentication and validation to deliver a dynamic, multi-layered, risk-based decisioning workflow that does not adversely impact the patient experience. LexisNexis Device Assessment provides:

1. A near real-time analysis and authentication of device and identity data
2. Risk scoring and pass/reject/review decisioning based on healthcare organization rules
3. A tailored authentication path assigned based on risk determination
4. Frictionless user experiences only sending questionable users down more intense levels of security

LexisNexis Device Assessment—the first layer of protection

LexisNexis Device Assessment leverages the industry's largest global device intelligence networks to score and authenticate devices and return risk attributes to inform onboarding and authentication decisions.

Transactions supported:

- Login
- New patient enrollment
- Account updates
- Post discharge care management
- Online payment

Device identity and location attributes for:

- Desktop computers
- Laptops
- Mobile phones
- Tablets

Real-time intelligence:

- Risk score
- Reason codes
- Risk classification
- Review status
- 200+ attributes

Integrating Device Assessment as a first layer of defense offers a wide range of advantages:

Fraud Reduction

- Reduces losses from fraud by enhancing patient and provider authentication
- Identifies stolen patient identities
- Pinpoints true locations behind hidden proxies and VPNs
- Exposes bots, malware and scripted attacks
- Blocks blacklisted fraudsters
- Increases effectiveness of other anti-fraud tools

Frictionless Authentication

- Increases returning device recognition
- Reduces step-up authentications for appropriate users
- Creates a stronger patient experience and establishes a trusted relationship quickly
- Minimizes false positives

Device Reporting

- Transactional and summary level activities
- Risk trend, score distribution, top attributes and rules triggered with configurable time period
- Run scheduled or recurring real-time reports
- Export data to create custom reports

Device Admin Portal

- Customize scoring parameters and escalation procedures depending on risk tolerance
- Receive real-time email alerts
- Queue risky transactions for manual review

By itself, Device Assessment is a highly effective initial layer of authentication, which is seamless and undetectable from a user perspective. Combined with additional layers of LexisNexis identity verification analytics, risk-based scoring and individualized authentication paths, Device Assessment is the springboard to an entirely new and holistic way of addressing the changing security, fraud and authentication environment.

To optimize your identity strategy, contact your local LexisNexis Health Care representative or call 866.396.7703 and ask about any LexisNexis Risk Defense products for healthcare:

- InstantID® Q&A
- Device Assessment
- TrueID®
- Instant Verify
- One Time Password
- FraudPoint®

LexisNexis® RISK SOLUTIONS | Health Care

About LexisNexis® Risk Solutions

At LexisNexis Risk Solutions, we believe in the power of data and advanced analytics for better risk management. With over 40 years of expertise, we are the trusted data analytics provider for organizations seeking actionable insights to manage risks and improve results while upholding the highest standards for security and privacy. Headquartered in metro Atlanta USA, LexisNexis Risk Solutions serves customers in more than 100 countries and is part of RELX Group plc, a global provider of information and analytics for professional and business customers across industries. For more information, please visit www.risk.lexisnexis.com.

Our healthcare solutions combine proprietary analytics, science and technology with the industry's leading sources of provider, member, claims and public records information to improve cost savings, health outcomes, data quality, compliance and exposure to fraud, waste and abuse.