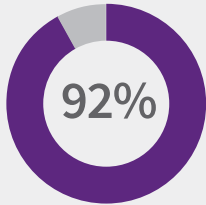




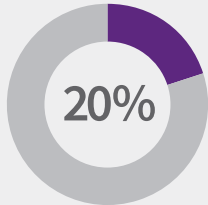
Leverage frictionless, real-time authentication to protect information when accessed via mobile devices

Increased global mobile device (i.e. cellular devices, tablets, laptops, etc.) usage to access health information has inevitably created expansive security vulnerabilities and attracted an increased volume and variety of cyber fraud. The need to maximize security while maintaining a positive member experience has fueled the evolution of a multi-layered approach to onboarding and authentication. LexisNexis® Device Assessment offers an ideal first layer of defense.

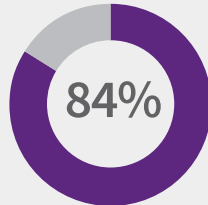
## Healthcare has gone mobile



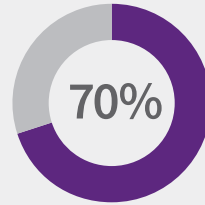
OF PATIENTS CAN ACCESS HEALTH RECORDS DIGITALLY VERSUS 43% JUST TWO YEARS PRIOR<sup>1</sup>



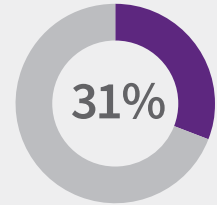
HIGHER RETENTION RATES FOR NEW PATIENTS THAT SIGN UP FOR A PORTAL ACCOUNT WITHIN 30 DAYS OF THEIR VISIT<sup>2</sup>



OF SURVEYED CARE PROVIDERS ARE USING MOBILE DEVICES; PRIMARILY TABLETS; FOR POST-HOSPITAL DISCHARGE SUPPORT<sup>3</sup>



OF SURVEYED DOCTORS USE MOBILE DEVICES TO MANAGE IN-PATIENT DATA<sup>4</sup>



OF PATIENTS HAVE USED A MOBILE APP TO COMMUNICATE WITH THEIR HEALTHCARE PROVIDER<sup>5</sup>



**Mobile has created a feeding frenzy of fraudulent activity:**

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

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

## Security and fluidity are a balancing act

One challenge of protecting patient data is the journey the data must take. In today's environment, highly personalized and comprehensive member data can travel through secure home networks, from devices to apps over the internet, to a more precarious journey through cloud or central repositories to reach physicians and health plans.

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

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

## LexisNexis Health Care has reinvented authentication

Delivering effective and efficient security requires a dynamic, multi-layered, risk-based decisioning workflow:

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. Step-up intensity and tailored authentication path assigned based on risk determination
4. Valid users experience no friction; questionable users traverse appropriate security levels

## 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 member 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 member and provider authentication
- Identifies stolen member 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 member 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 to address 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®



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](http://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.

Device Assessment, InstantID Q&A, TrueID, Instant Verify, One Time Password and FraudPoint provided by LexisNexis are not provided by "consumer reporting agencies" as that term is defined in the Fair Credit Reporting Act (15 U.S.C. § 1681, et seq.) ("FCRA") and do not constitute a "consumer report" as that term is defined in the FCRA. Device Assessment, InstantID Q&A, TrueID, Instant Verify, One Time Password and FraudPoint may not be used in whole or in part as a factor in determining eligibility for credit, insurance, or employment or for any other eligibility purpose that would qualify it as a consumer report under the FCRA. Due to the nature and origin of public record information, the public records and commercially available data sources used in reports may contain errors. Source data is sometimes reported or entered inaccurately, processed poorly or incorrectly, and is generally not free from defect. This product or service aggregates and reports data, as provided by the public records and commercially available data sources, and is not the source of the data, nor is it a comprehensive compilation of the data. Before relying on any data, it should be independently verified. LexisNexis and the Knowledge Burst logo are registered trademarks of RELX Inc. Copyright © 2017 LexisNexis. All rights reserved. NXR12181-00-1017-EN-US