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

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

Mobile has created a feeding frenzy of fraudulent activity:

• BOT activity is in an uptrend, after a three-year decline
• Medical identity theft and big data breaches in the medical industry have been on the rise
• 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

Healthcare has gone mobile:

- 92% of patients can access health records digitally versus 43% just two years prior
- 20% higher retention rates for new patients that sign up for a portal account within 30 days of their visit
- 84% of surveyed care providers are using mobile devices; primarily tablets; for post-hospital discharge support
- 70% of surveyed doctors use mobile devices to manage in-patient data
- 31% of patients have used a mobile app to communicate with their healthcare provider
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®