mcol

LexisNexis® RISK SOLUTIONS | Health Care

EXECUTIVE REPORT

Health Plan Cybersecurity Trends and Risk Management Response Preparations

2020

Business is booming for cybercrooks.
The frequency of breaches continues to rise every year across all industry sectors.
So does the cost for each company that suffers a cyberattack.

Healthcare sits at the top of the victim list.

This report, sponsored by LexisNexis Risk Solutions, examines the impact of the growing number of cyberattacks and reflects on the current state of healthcare cybersecurity concerns among health plans and other key healthcare stakeholders.

Despite cybersecurity spending increasing 8% during the past year, the health industry continues to experience a record number of cyber threats. The payer market will be impacted by new regulations around interoperability and patient access rules that require more patient data to be moved via API, which can create more vulnerability. This may cause additional interoperability impediments in the processes for detection, reporting and remediation of cyberbreaches. The responsibility will lie with health plans to balance interoperability (data sharing) and data security.

The numbers associated with security breaches are grim.

- IBM Security's *2020 Cost of a Data Breach Report* finds that breaches cost companies $3.86 million a pop, on average. Compromised employee accounts are the most expensive root cause, IBM adds, and 80% of the incidents expose Personally Identifiable Information.
- In healthcare, the average cost of a data breach in 2020 is almost twice the overall average, at $7.13 million, IBM says, placing it atop the list of 17 industries surveyed. Not to mention, "the average time to identify and contain a breach in healthcare is 329 days."
- The *Verizon Data Breach Investigations Report 2019* confirmed that 15% of all breaches involve healthcare companies, and that 71% are financially motivated. Two-thirds are perpetuated by outsiders, but 34% of cyberthieves are insiders, the report adds, noting, like the IBM report does, that 56% of the breaches take more than 60 days to detect.
- The Ponemon Institute's *2019 Cost of Data Breach Study* says breaches average $429 per record.

And the environment is getting murkier and spookier.

- *Identity thieves use the PII they steal to get credit and buy things, or take out loans, or commit IRS tax return fraud or file false medical claims. What they don't use themselves, they move on the Internet black market, where they can anonymously sell to the highest bidder.*
- *Typically, PII is sold in huge batches, hundreds of thousands at a time; recent rates for name, Social Security Number and date of birth range up to $1.50 per record, while medical notes and prescriptions can easily fetch $20 apiece. Stealing and selling one hundred thousand medical records from a big payer can translate to $2 million dollars to the cybercriminal.*
- *Automated hacking is on the rise, says Alaap B. Shah, a member of the firm Epstein Becker Green PC, Washington DC, and presenter at a recent webinar on Health Plan cybersecurity trends & risk management response preparation. Indeed, he reported, humans now account for less than half of committed cybercrimes – and ransomware attacks, which hold data hostage until a ransom payment is made, are becoming widespread. Much of the "rampant cyberextortion in the healthcare sector," he adds, is carried out through phishing attacks.*
- *According to Shah, some of the key attackers are state governments outside the US. "Healthcare continues to be targeted by Russian- and Chinese-affiliated adversaries," Shah warns, noting that key adversaries also originate from North Korea, Eastern Europe and the Middle East.*

40% of health plans and other stakeholders expect to increase their security related budget for 2020/2021.

LexisNexis Risk Solutions, a provider of data and advanced analytics that helps healthcare organizations reduce risk and improve decisions, partnered with MCOL to gain a general impression of healthcare stakeholder perceptions on cybersecurity issues. MCOL surveyed selected participants, attending an online session on healthcare cybersecurity or responding to an online invitation. The survey considered six healthcare cybersecurity issues:

- Current Security Risks
- Drivers that cause organizations to Sacrifice Security
- Roles responsible for Identity & Access Management
- Identity & Access Management Budget Allocation
- 2020/2021 Budget Expectations
- Confidence in Current Authentication Measures

A summary of findings from stakeholder participants follows:

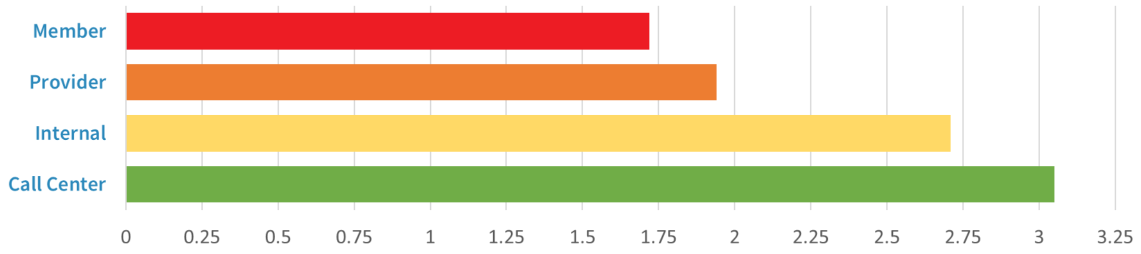
Ranking Security Risks

Rank the following four security risks that your organization is most concerned with, with 1 being the highest risk and 4 being the lowest

- *Internal employee hack/unauthorized access*
- *External attack via a provider portal or other third-party vendor*
- *External hacker attack on member portal or mobile application*
- *Attack via a Call Center*

Security Risk of Most Concern to Health Plans

(1- Highest Risk | 4 = Lowest Risk)



Avg. Score	Internal	Provider	Member	Call Center
Health Plan	2.71	1.94	1.72	2.18
All others	2.24	1.90	1.87	3.05
Total	2.38	1.91	1.82	2.79

(Lower avg score = higher risk, higher avg. score = lower risk; 1= highest, 4 = lowest)

An equal percentage of health plans (38.9%) found Provider and Member portal attacks the highest-risk; few plans considered internal attacks as the highest-risk (5.6%).

% Ranking Highest (1)	Internal	Provider	Member	Call Center
Health Plan	5.6%	38.9%	38.9%	16.7%
All others	22.9%	17.1%	45.7%	14.3%
Total	17.0%	24.5%	43.4%	15.1%

Drivers to Reassess Security Priorities

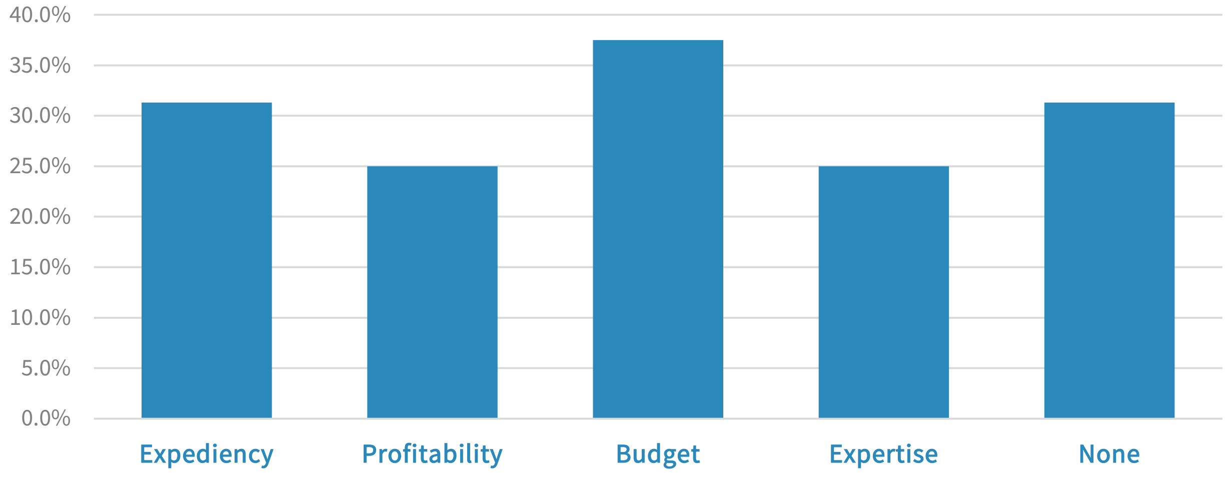
Which of the following might drive your organization to reprioritize certain security measures? (check all that apply)

- ■ *Expediency/Convenience*
- ■ *Profitability Targets*
- ■ *Lack of Budget*
- ■ *Lack of Expertise*
- ■ *None of the Above*

Health plans and other stakeholders were fairly closely aligned in their consideration of these drivers. More than one-third (35%) felt none of these drivers would cause them to sacrifice security.

% Listing	Expediency	Profitability	Budget	Expertise	None
Health Plan	31.3%	25.0%	37.5%	25.0%	31.3%
All others	28.6%	22.9%	42.9%	22.9%	37.1%
Total	29.4%	23.5%	41.2%	23.5%	35.3%

Drivers to Reprioritize Security at Health Plans



Responsibility for Identity & Access Management

Who has responsibility for Identity & Access Management (IAM) in your organization? (check all that apply):

■ *IT department*

■ *Health information management*

■ *Compliance or risk management*

■ *Privacy department*

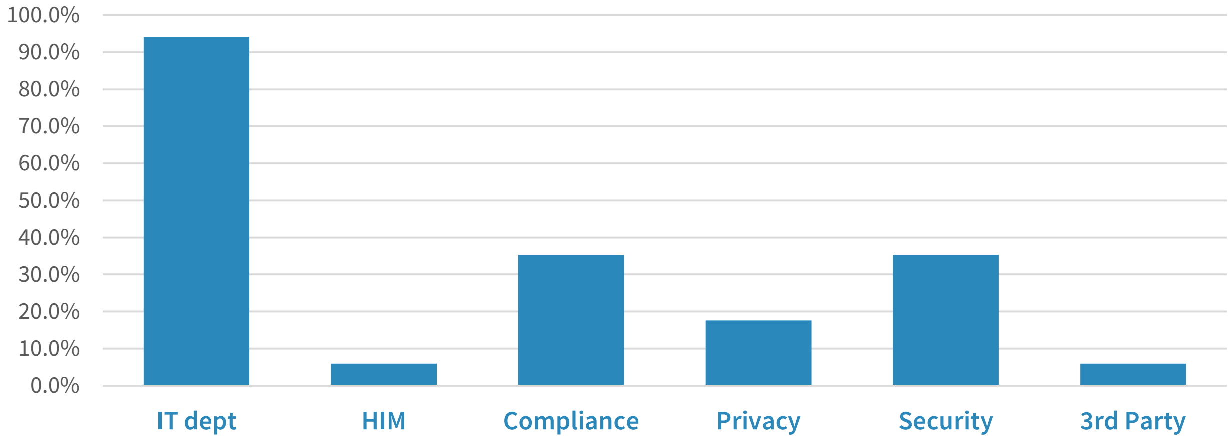
■ *Security organization*

■ *Third-party vendor*

Health plans and other stakeholders were aligned in agreement (both over 90%) that IT departments had the predominant responsibility for IAM, and they were aligned in the portion (35% and 37% respectively) that allocated responsibility to security organizations. Health plans did not spread responsibilities around in other listed areas as frequently as other stakeholders.

% Listing:	IT dept	HIM	Compliance	Privacy	Security	3rd Party
Health Plan	94.1%	5.9%	35.3%	17.6%	35.3%	5.9%
All Others	91.4%	20.0%	54.3%	25.7%	37.1%	11.4%
Total	92.3%	15.4%	48.1%	23.1%	36.5%	9.6%

IAM Responsibilities at Health Plans



Identity & Access Management Budget Allocation

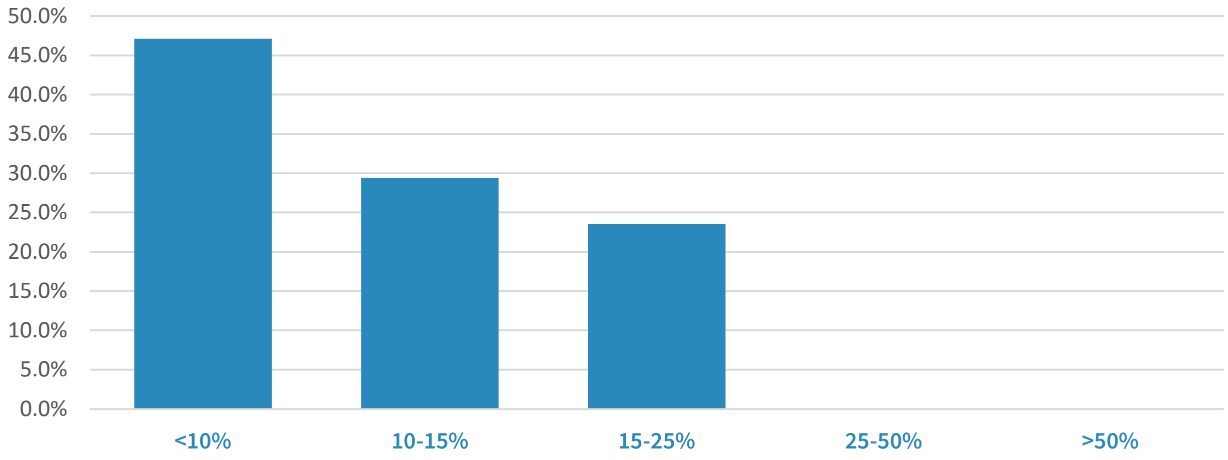
What percentage of your cybersecurity budget goes to Identity & Access Management annually?

- 🟦 *Less than 10%*
- 🟦 *10-15%*
- 🟦 *15-25%*
- 🟦 *25-50%*
- 🟦 *More than 50%*

75% of stakeholders allocate less than 15% of their budget for IAM, with 40% allocating under 10%. No participating health plans allocated over 25%.

% of Budget:	<10%	10-15%	15-25%	25-50%	>50%
Health Plan	47.1%	29.4%	23.5%	0.0%	0.0%
All others	37.1%	37.1%	14.3%	8.6%	2.9%
Total	40.4%	34.6%	17.3%	5.8%	1.9%

Percentage of Budget for IAM at Health Plans



2020/2021 Budget Expectations

For 2020/2021, is your budget expected to:

■ *Increase significantly*

■ *Increase slightly*

■ *Stay the same*

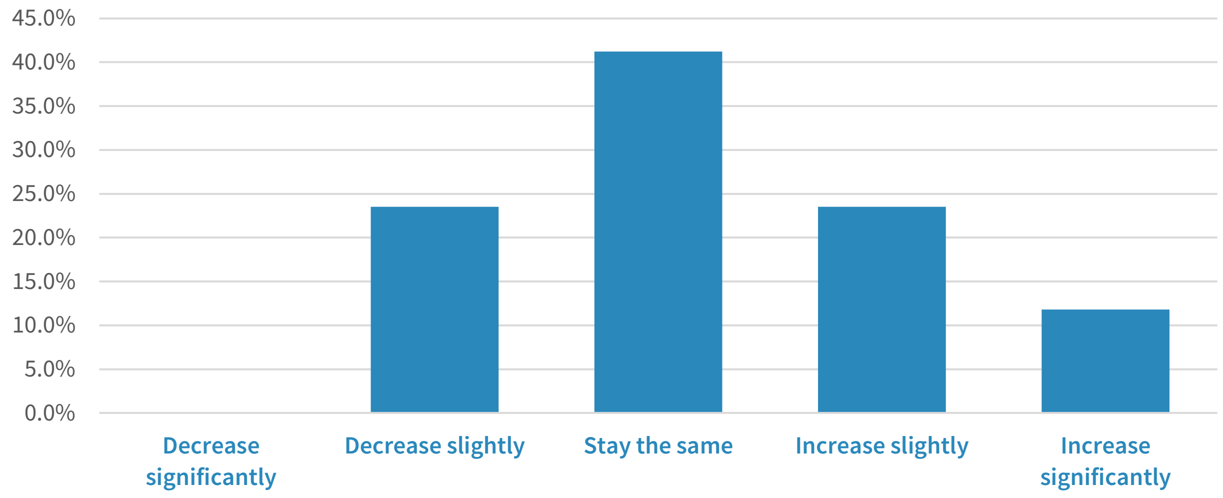
■ *Decrease slightly*

■ *Decrease significantly*

Approximately 40% of stakeholders expect their budgets to stay the same, 40% expect their budgets to increase and 20% expect a decrease. Health plans were more pessimistic, with 23.5% expecting a decrease compared to 17.2% of other stakeholders.

Budget Expectation	Decrease significantly	Decrease slightly	Stay the same	Increase slightly	Increase significantly
Health Plan	0.0%	23.5%	41.2%	23.5%	11.8%
All others	2.9%	14.3%	40.0%	31.4%	11.4%
Total	1.9%	17.3%	40.4%	28.8%	11.5%

2020 / 2021 Budget Expectations at Health Plans



Confidence in Current Authentication Measures

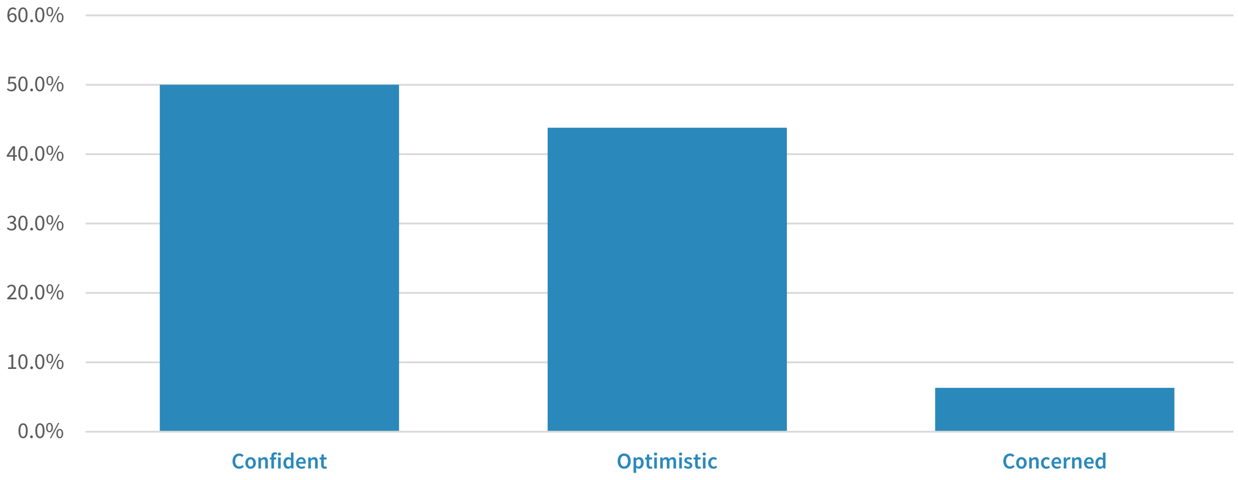
What is your level of confidence in your current authentication measures to prevent unauthorized access to valuable information via patient and/or provider portal or mobile application? (Choose from one of these three scenarios):

- *Confident – we have the necessary controls in place and audit both ourselves and our vendors regularly, and we have not detected a breach*
- *Cautiously optimistic – we (and our partners) have some controls in place and have not detected a breach, but realize we could add more controls*
- *Concerned – our (or our vendor partners') controls are outdated and we are in the mindset of "It's not if, but when, we will experience a breach"*

Only 6% of health plan respondents categorized their response as "concerned." On the other hand, more health plans (50%) were "confident" compared to other stakeholders (42%).

Response:	Confident	Optimistic	Concerned
Health Plan	50.0%	43.8%	6.3%
All others	41.9%	54.8%	3.2%
Total	44.7%	51.1%	4.3%

Health Plan Confidence Level in Current Authentication Measures



94%

of health plan respondents indicated that IT departments were responsible for Identity & Access Management within their organizations.

> "There is significant variation among health plans in the assignment of the 'privacy officer' role and, more broadly, in assigning responsibility for the organization's strategies, philosophy, policies and procedures regarding Identity & Access Management. Sometimes, such non-technical responsibilities are assigned to the CIO, sometimes to business operations executives and sometimes to legal and risk management professionals."
>
> -Richard E. Ward MD MBA, Senior Advisor at BDC Advisors

HIPAA's Demands Drive Many Payers' Cybersecurity Strategies

Health payers are "required by HIPAA regulations – and contractually committed in many network agreements – to designate an executive to serve as the privacy officer to take responsibility for assuring the security and confidentiality of protected health information," notes Richard E. Ward MD MBA, Senior Advisor at BDC Advisors. But, he adds, "there are no regulatory limits on which executives can take on that responsibility, and there is significant variation among health plans in the assignment of the role and, more broadly, in assigning responsibility for the organization's strategies, philosophy and policies & procedures regarding IAM."

- *IT "almost always takes responsibility for the technical aspects of data security and application access management," Ward adds, including network security, encryption of data in motion and at rest and overseeing the directory technology used to manage user accounts and associated data and application privileges.*
- *But "sometimes, such non-technical responsibilities are assigned to the CIO," he explains, "sometimes to business operations and sometimes to legal and risk management professionals."*
- *Any of those positions can handle the function, but when legal or technology professionals take the reins, he says, "there can be a tendency for data policies to prioritize risk avoidance, which can reduce the ability of the organization to pursue healthcare analytics and cross-network data sharing with agility and nuance."*

Whoever captains the ship, the path to data security has to include a robust governance structure that includes an Enterprise Risk Management Committee to adopt ERM policy at an organization and at a Board level. The Board's role includes both a "duty of care," to "act on an informed basis and in good faith," Shah notes, and a "duty of oversight," to "ensure there's a system in place monitoring activity."

Data safety also includes regular risk assessments – that don't indulge anyone's paranoid delusions. Healthcare companies can also beef up policies regarding which devices can be connected to the network, make sure assets reside behind a well-configured firewall and segment the network to prevent attackers from pivoting across systems.

With growth in interoperability – sharing of data, comes an increase in vulnerabilities. LexisNexis Risk Solutions has a solution to assist with balancing member engagement and data security for both members and employees across channel.

LexisNexis provides a Multi-factor Authentication to help healthcare organizations assess the risk of both physical and digital identity attributes. This approach allows health plans to balance both security and ease of use and delivers high predictive identity intelligence and fraud decisioning tools to position health plans for critical success.

Accelerate identity verifications	Integrates easily with existing business processes and can be customized to fit your workflow.
Streamline access decisions	Leverage identity intelligence to confirm and authenticate members throughout the member life cycle.
Protect against identity fraud	Swiftly confirm that your members and providers are who they claim to be.
Enhance member portal security	Authenticate a user through at least two independent elements.

Sources:

- Symantec's Internet Security Threat Report 2019: https://docs.broadcom.com/doc/istr-24-2019-en
- https://www.forbes.com/sites/rogeraitken/2018/08/19/global-information-security-spending-to-exceed-124b-in-2019-privacy-concerns-driving-demand/?sh=2b3e83117112
- https://www.gartner.com/en/newsroom/press-releases/2018-08-15-gartner-forecasts-worldwide-information-security-spending-to-exceed-124-billion-in-2019
- https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/
- https://enterprise.verizon.com/resources/reports/dbir/
- https://content.govdelivery.com/attachments/USDHSCIKR/2019/04/16/file_attachments/1193648/HC3%20-%20HPH%20Breach%20Cost%20whitepaper.pdf
- https://enterprise.verizon.com/resources/reports/dbir/2019/summary-of-findings
- CrowdStrike: Observations From the Front Lines of Threat Hunting -- Overwatch 2019 Mid-Year Report
- FireEye: World War C: Understanding Nation-State Motives Behind Today's Advanced Cyber Attacks
- https://cyberinsureone.com/how-it-works/cost/
- https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf
- Care Analytics News: Intervention Edition, July 2020
- http://www.mcolblog.com/kcblog/2020/7/31/data-breaches-unfortunately-healthcare-is-the-leading-indust.html
- Health Plan Cybersecurity Trends and Risk Management Response Preparations – A HealthcareWebSummit Webinar, August 2020
- Stakeholder Perceptions on Healthcare Cybersecurity Concerns Survey conducted during the second and third quarters of 2020 from 58 representative stakeholder organizations, including 31% from health plans, and the balance from health systems, provider organizations and other healthcare stakeholder organizations

LexisNexis®
RISK SOLUTIONS

About LexisNexis® Risk Solutions

LexisNexis Risk Solutions harnesses the power of data and advanced analytics to provide insights that help businesses and governmental entities reduce risk and improve decisions to benefit people around the globe. We provide data and technology solutions for a wide range of industries including insurance, financial services, healthcare and government. 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 and www.relx.com.

The healthcare business of LexisNexis Risk Solutions has mastered the art of combining, analyzing and delivering data and analytics to optimize quality, performance, and impact across health care entities. Our solutions leverage the industry's most robust and accurate provider data, comprehensive public records, proprietary linking and claims analytics, predictive science, and computing platform to transform the business of healthcare.

This report is provided solely for general informational purposes and presents only summary discussions of the topics discussed. This report does not represent legal advice as to any factual situation; nor does it represent an undertaking to keep readers advised of all relevant developments. Readers should consult their attorneys, compliance departments and other professional advisors about any questions they may have as to the subject matter of this white paper. LexisNexis and the Knowledge Burst logo are registered trademarks of RELX Inc. Other products and services may be trademarks or registered trademarks of their respective companies.