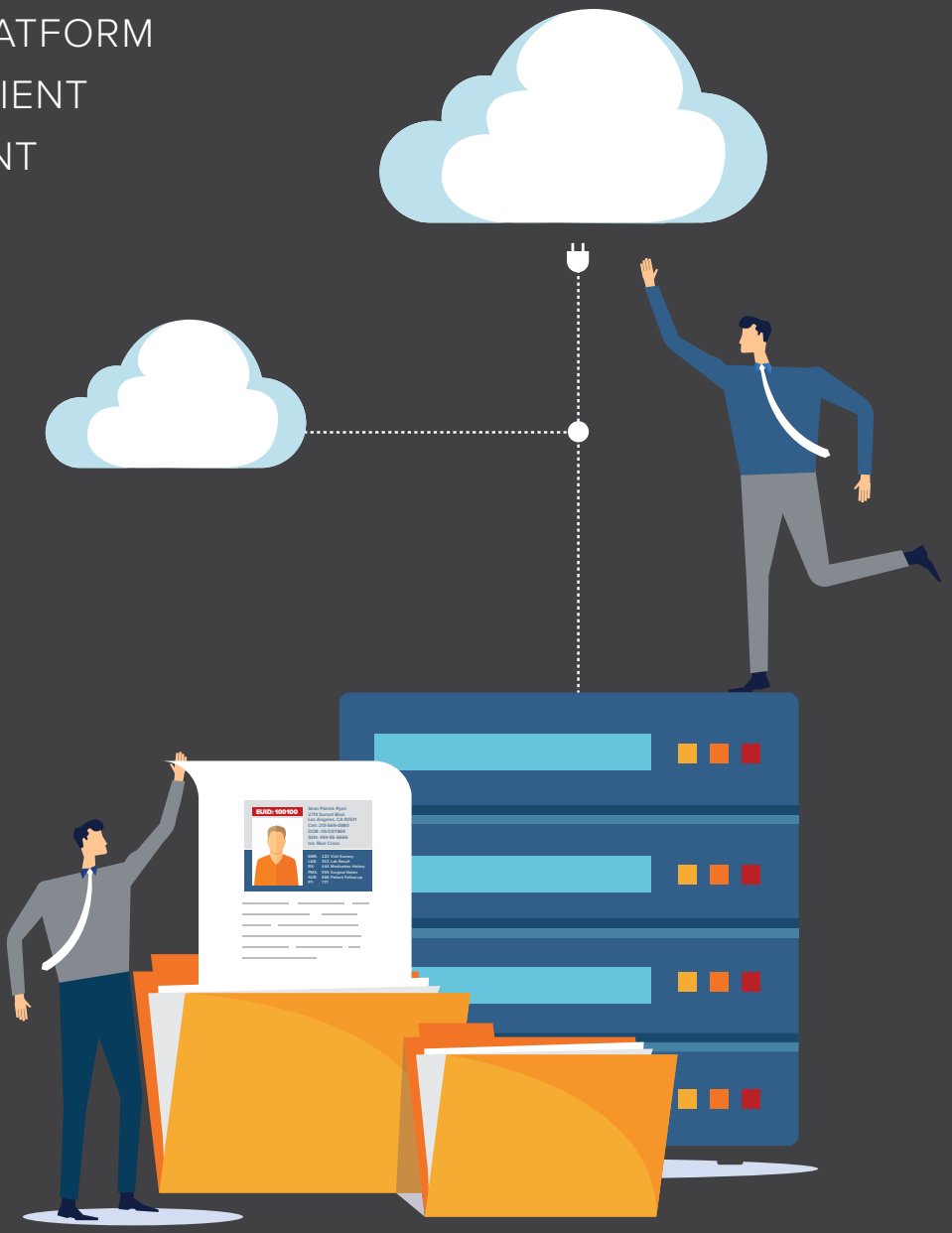
NEXTGATE

WHITE PAPER

Moving Patient Matching Capabilities to the Cloud:

HOW A CLOUD PLATFORM CAN IMPROVE PATIENT DATA MANAGEMENT



Overview

Moving patient identification and data matching functions to a cloud-based EMPI simplifies and strengthens the ability to share accurate and complete patient data.

The healthcare industry has long relied on legacy systems and on-premise computing power to ensure that patient data was secure and the idea of storing sensitive healthcare data in a nebulous "cloud" seemed preposterous just a decade ago.

Today, the healthcare industry is much more comfortable moving its data and applications to a cloud platform. Consumer acceptance of cloud offerings has grown exponentially in conjunction with universal adoption of smartphones and mobile apps, critical to their daily lives. Healthcare is following: according to the HIMSS 2016 Survey, 84% of healthcare providers are currently using a cloud service.[1]

The benefits of moving to the cloud include reduced costs, the ability to manage exponentially increasing data volumes without capital expenditures for infrastructure and human resources, the accessibility of data from any internet-connected device, reduced or eliminated downtime, increased data security, and the promise of data driven healthcare. And as healthcare organizations seek to manage the volume, velocity, and variety of patient data and eliminate duplicate records, the need for the scalability and data security of the cloud increases.

Value-based care and population health initiatives are gaining momentum and healthcare organizations are increasingly exchanging data to support these programs. Even though interoperability standards exist, sharing data seamlessly across systems and organizations remains a challenge and is exacerbated by the multiple records and identifiers that a patient can have within the various sites encountered in care delivery.

Identifying all the records related to the same patient is essential to efficient data exchange and patient safety. Moving patient identification and data matching functions to a cloud-based EMPI simplifies and strengthens the ability to share accurate and complete patient data.

CHALLENGE 1:

Patient Data Needs to be Integrated from Various Systems During M&A

We've entered the era of data-driven healthcare and with it, organizations need to aggregate, analyze, and secure huge datasets from various sources. For example, in an effort to build scale and new capabilities and remain competitive, healthcare organizations are increasingly coming together to create multi-region and multi-business unit organizations, according to Kaufman Hall.[2]

These organizations are combining huge datasets. Some studies estimate that volumes of medical data will increase 48% each year. IDC predicts the healthcare industry will have generated 2,314 exabytes (an exabyte is equal to about one billion gigabytes) by 2020.[3]

While mergers and acquisitions can play a significant role in how organizations approach value-based care and population health, integrating patient data from newly acquired medical groups, outpatient clinics, affiliated subsidiaries, and hospitals is challenging and wrought with errors. Multiple systems containing patient related data need to be integrated quickly into a format that the newly created organization can use. Combining data with different local identifiers increases the chances of misidentification and duplicate records, significantly impacting the value of the M&A.

To achieve the promise of data-driven healthcare, organizations need to ensure the integrity of these vast data stores. Data analytics can improve quality of care as well as uncover waste, but the data – all of it – needs to be related to the right patient so as not to skew results.

CHALLENGE 2:

Exploitation of Security Vulnerabilities is on the Rise

One of the most talked about security challenges in healthcare is medical identity fraud. A study from the Ponemon Institute finds that 2.32 million Americans have been victims of medical identity theft and 65% of those victims spent an average of $13,500 and more than 200 hours to undo the mess.[4]

But identity fraud is not the only security vulnerability that hackers and criminals are exploiting. Another hot area is ransomware in which cybercriminals hold data hostage until the ransom is paid. ECRI Institute names ransomware the top health technology hazard for 2018.[5]

Additionally, HIPAA enforcement over data breaches is increasing, with some of the largest monetary penalties from the Office for Civil Rights

(OCR) enforcement occurring in 2017. HIPAA requires that all protected health information (PHI) under U.S. law, whether electronic, on paper, or oral, be encrypted and secured.

Healthcare organizations are fighting back—but it's costly: 71% are allocating part of their IT budget specifically to cybersecurity, reports the 2017 HIMSS Cybersecurity Study.[6]

And it's likely that they don't have the resources they need to stay-up-to-date with the latest threats and adequately protect their organizations. Security resources are stretched thin and it's difficult to allocate the staff for security monitoring, performing vulnerability scans, and maintaining HIPAA security minimums.

CHALLENGE 3:

The Cost of Maintaining an On-Premise Patient Matching Solution

IT continues to be an expensive cost center and capital expenditures for hardware and software are just the beginning. Healthcare organizations must employ highly paid IT professionals to keep the IT lights on, manage upgrades, integrate new technologies, keep up with storage demands, and ensure data security and privacy that meets regulatory scrutiny at the same time they are struggling to further quality of care initiatives.

Maintaining an on-premise patient matching solution requires all of the above, as well as subject matter experts on the application itself.

Healthcare organizations are desperate to reduce infrastructure costs, and many are looking to the cloud. According to a recently released survey by KLAS, 70% of healthcare organizations have moved at least some applications or IT infrastructure off premises.[7] A recent Riverbed survey found that 90% of IT decision-makers agree that legacy network infrastructure cannot keep up with the demands of the modern network infrastructure.[8]

The Right Cloud for Patient Matching

With sophisticated evaluation of patient records, a cloud-based enterprise master patient index (EMPI) provides healthcare organizations with access to data that leads to better care, more accurate clinical decision-making, and less waste due to inefficiencies. Because the cloud can ingest and process infinite amounts of data, it can manage the huge volume of patient records and handle the demands of an EMPI cost effectively and efficiently. The cloud can determine duplicates and generate an Enterprise Identifier that can be used by all enterprise systems.

The demands for IT talent ebb and flow. Since 8% to 12% of patient records are duplicates, an EMPI data upload requires cleanup.[9] Onboarding new data sources due to mergers and acquisitions or organizational restructuring requires IT resources. Rather than hiring and training additional staff, organizations are turning to a managed service provider (MSP) to handle these spikes in staffing and resource requirements. The cloud vendor manages upgrades and ongoing maintenance, so the healthcare organization can reduce staffing requirements.

But not all cloud providers address the unique challenges faced by the healthcare industry. To ensure patient data is safe, a cloud provider should implement data encryption both when data is in transit and when it is at rest, firewalls, multifactor authentication, vulnerability scanning, intrusion detection and prevention, application level security, and strict access management controls.

By off-loading EMPI to the cloud, the organization relies on the cloud vendor to provide the security fence and continuous monitoring. While the largest cloud providers, including Amazon Web Services, Microsoft Azure, Google, and IBM, have extensive security controls, each differs in their approach. Make sure you understand how the providers address both physical security of their data centers as well as governance and controls to comply with regulations such as HIPAA.

By moving EMPI to the cloud, healthcare professionals, relieved of the day-to-day maintenance of on premise, can focus on data management that furthers value-based healthcare, patient engagement, and risk-based initiatives. Time spent on incident management, change management, release and deployment, and impact issues can be reallocated to population health programs. The result is significantly improved patient outcomes for less cost.

By moving EMPI to the cloud, healthcare professionals, relieved of the day-to-day maintenance of on premise, can focus on data management that furthers value-based healthcare, patient engagement, and risk-based initiatives.

References

1. https://www.cleardata.com/wp-content/uploads/2016/12/2016-HIMSS-Analytics-Cloud-Study.pdf
2. https://www.kaufmanhall.com/news/hospital-merger-and-acquisition-activity-pace-potentially-exceed-2016-according-kaufman-hall
3. https://med.stanford.edu/content/dam/sm/sm-news/documents/StanfordMedicineHealthTrendsWhitePaper2017.pdf
4. http://medidfraud.org/wp-content/uploads/2015/02/2014_Medical_ID_Theft_Study1.pdf
5. https://www.ecri.org/press/Pages/ECRI-Institute-Release-2018-Top-Hazards-List.aspx
6. http://www.himss.org/sites/himssorg/files/2017-HIMSS-Cybersecurity-Survey-Final-Report.pdf
7. https://klasresearch.com/report/off-premises-computing-perception-2017/1193
8. https://www.riverbed.com/gb/press-releases/riverbed-future-of-networking-survey-finds-legacy-networks-holding-back-cloud-and-digital-transformation.html
9. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4832129/

ABOUT NEXTGATE

NextGate is the leading provider of identity matching solutions that connect the healthcare ecosystem to help organizations promote interoperability and overcome the clinical, operational and financial challenges that result from duplicate records and siloed systems enabling seamless data exchange, enhanced clinical decision-making and value-driven care. **For more information, visit www.NextGate.com.**