



Unique Health Safety Identifier Across The Continuum of Care

Andy Nieto, Health Solutions Executive



@ALN669

Trend

Longer Life

Average life expectancy in OECD countries in 2012 was **80 YEARS**, an increase of 5 years since 1990. ¹



Physicians Shortage

Shortage of **13.7k physicians in 2010** and projected to be well above **140k** or about **19%** fewer doctors than are needed **by 2025**, in US. ³ shortage of more than 4 million doctors, nurses, midwives and others ⁴



More Aging

Meet the over 65s – by 2018 – **10% of the global population.** ²



- World Is Facing A -
Challenging Future
- In -
Healthcare

Higher Cost

Growth in average annual **healthcare spending** 2014 - 2018 is expected to range from **2.4%** in **Western Europe** to **4.9% North America**; and from **8.1%** in **Asia** and **Australia** to **8.7%** in the **Middle East** and **Africa.** ²



Rising Chronic Disease

The number of people with **diabetes** globally is **382 million**, around **98 million (25.7%)** are Chinese. ²

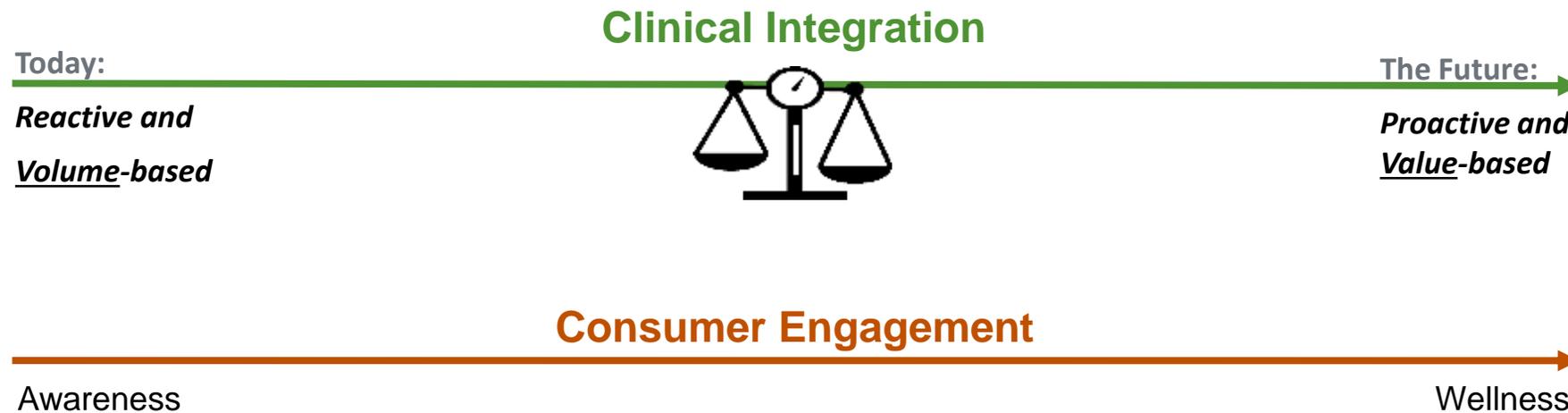


Growing Population

Global population has grown from **1 billion** in 1800 to **7 billion** in 2012, and projected to 8.4 billion by mid-2030, and **9.6 billion** by mid-2050. ⁴



Health Plus Care Transformation



Problems

Do these challenges impact your clinical and financial operations?

Duplicate Records

skew patient population metrics and put patients at risk for medical errors and inappropriate treatment.

- On average, an excess of 10% of medical records are duplicates, per facility or network system
- ONC's objective is to reduce that rate down to 2% by 2017, 0.5% by 2020, and 0.1% by 2024

Medical Identity Theft

compromises PHI and patient safety—over 250,000 lives are lost every year due to medical errors.

- Costs the United States \$84 billion a year
- In 2014, medical identity theft victims paid \$20 million out-of-pocket

Payment Fraud

is a major factor in revenue loss—tens of billions in revenue loss.

- \$272 billion is lost to healthcare fraud and abuse within Medicare and Medicaid programs alone
- Sixty-two percent of finance professionals report that their organizations were targets of payment fraud in 2014. This has translated to nearly \$28 Billion in overall cost (out of pocket expense plus the cost of overall services);

Medical Identity Theft – Who Are You?

- Cost Impact
 - \$84 Billion a year problem
- Data Security
 - In 2014, nearly 9 million patient health records were breached in 164 reported incidents.
 - By March 2015 some 90 million patients were affected.
 - In one incident the Social Security Number (SSN) of 79 million individuals was compromised.

Duplicate Records

- Each EHR and HIE leverages an EMPI solution yet an alarming statistic that Health IT systems contain 8% to 12% of duplicate medical records. ²
- The American Health Information Management Association (AHIMA) emphasizes that misidentification and duplicate information entered into electronic health records (EHRs) cause misdiagnoses, unnecessary tests, and inappropriate treatments, all of which hinders the ability to improve patient care and drives up medical costs. ³
- According to the Office of the National Coordinator for Health Information Technology (ONC), accurate patient identification is the single largest roadblock to true interoperability. ⁴
 - ONC Interoperability Roadmap call for all organizations that match electronic health information have an internal duplicate record rate of no more than 2% at the end of 2017. ⁵
- MACRA requires us to remove Social Security Numbers (SSNs) from all Medicare cards.

Source

2. AHIMA Foundation, Perspectives in Health Information Management, Why Patient Matching Is a Challenge: Research on Master Patient Index (MPI) Data Discrepancies in Key Identifying Fields, Spring 2016
3. [Petition Calls for Unique Patient Identifier Solution](#). Journal of AHIMA. March 21, 2016.
4. [Patient Matching and Identification Report](#). The Office of the National Coordinator for Health Information Technology. February 7, 2014.
5. [Connecting Health and Care for the Nation: A Shared Nationwide Interoperability Roadmap Final](#). Version 1.0, Office of National Coordinator, October 6, 2015

Financial Impact Due to Duplicate Electronic Records

- Duplicates in the range of 8% to 12% erodes confidence in the data and lead to unnecessary and costly clinician and HIM Verification activity.
- As hospital have information, duplicates and overlays will grow exponentially.
 - The rise of Integrated Delivery Network (IDNs) and Health Information Exchanges (HIEs) is exponentially increasing the size of enterprise master patient indexes (EMPIs) from desperate sources causing more overlays and duplicates.
- According to Fox and Sheridan, the Average cost of a duplicate medical record pair is \$50.
- Correcting a paper-based overlay patient record can take 60 to 100 hours
- In an EHR environment the time to fix an overlay can take months depending on the complexity of the system.

The Limitation of Enterprise Master Patient Index (EMPI)

- Historically Approach

- the way to address this issue of identity disambiguation is through the use of Enterprise Master Patient Index (EMPI) technology

- Limitations

- Attributes matching and scoring hits a theoretical limit of 98% accuracy
 - a level only achieved when the patient demographic record has a complete set of details with strong data governance policies.
- Challenged to detect medical identity theft; leading to corruption of the patient record;
- If unable to find an existing patient (based on search criteria) the EMPI facilitates an EHR to create a new patient and store information in an unrelated record.

Payment Fraud

- Payment Fraud is a by-product of identity theft – a misrepresentation of whom one is and/or proper identity yet providing unauthorized forms of payment.
- Consumers bearing a greater burden of the cost of care, last year alone, consumers spent \$824 billion for healthcare services including out of pocket and deductible payments. This spending trend is expected to reach \$2 Trillion by 2020.
- Sixty-two percent of finance professionals report that their organizations were targets of payment fraud in 2014. ⁶ This has translated to nearly \$28 Billion in overall cost (out of pocket expense plus the cost of overall services);
- Payment for services should not be looked at separately from Medical Identity Theft.

Source:

6 2015 AFP Payments fraud and Control Survey, Underwritten by J.P.Morgan, March 2015

Challenge Summary

- Medical Identity Theft, Duplicate Records, Payment Fraud have been long standing problems in the care delivery model.
- Many have implemented data reconciliation processes that merge records without awareness nor detection of medical identity theft – potentially causing harm to innocent patients.
 - Other collect biometrics from patients without identity proofing them employing recommended NIST LoA3 criteria while also using processes and trained resources from an accredited EHNAC (The Electronic Healthcare Network Accreditation Commission) Registration Authority;
- Most only identity proof a consumer patient within the silo of a specific delivery of care facility – while continuing to maintain different identities and demographic details across the multiple care settings.

Pivoting to Support a Value Based Care Delivery

- The solution cannot be solved by one EHR vendor
- It requires a unique shared approach recognized by all.
 - Implementing a Unique Health Safety Identifier (UHSI) coupled with multi-factor authentication while validated under the guides of an EHNAC accredited registration authority is known to eliminate medical identity theft, duplicate records and payment fraud
 - Only when this UHSI is used across the continuum of care can confidence be restored to the data quality
- Once eliminating these long standing challenges it will lead to improved data quality at the point of care.
- Provide value based care delivery providing the true data set necessary to manage the lives within their care.

Not Just a Data Issue

- Patient Satisfaction
- Personalization and recognition improves outcomes

Industry Comments About the Need for Accurate Identity?



“**Accurate patient identification** is foundational to the successful linking of patient records within care delivery sites and across the healthcare ecosystem to underpin care delivery, data exchange, analytics, and critical business and clinical processes.”

AHIMA

“The ultimate goal is the **accurate identification** of the patient and linking of all related information to that individual within and across systems. Linking the wrong clinical information to a person can not only cause great personal harm to the patient, but can also incur huge costs to the healthcare provider in correcting and mitigating the error.”

HIMSS

“**Accurate identification** can greatly reduce the risk of preventable medical errors and significantly increase quality of care. It can also drive out unnecessary costs by reducing inefficiency. An identification system done well can protect a patient’s identity and privacy much better than the current system. First and foremost, patient identification is about patient safety, and we need to get it 100% right the first time, and every time.”

CHIME

“MIFA’s singular focus is on what has emerged in recent years as a significant and deeply personal healthcare threat – medical identity fraud. Our mission is to galvanize all stakeholders in the healthcare industry around awareness, prevention, detection and remediation. **Medical identity theft** isn’t just a financial threat – it’s also clinical – and it has a much longer timeline than other forms of identity theft.”

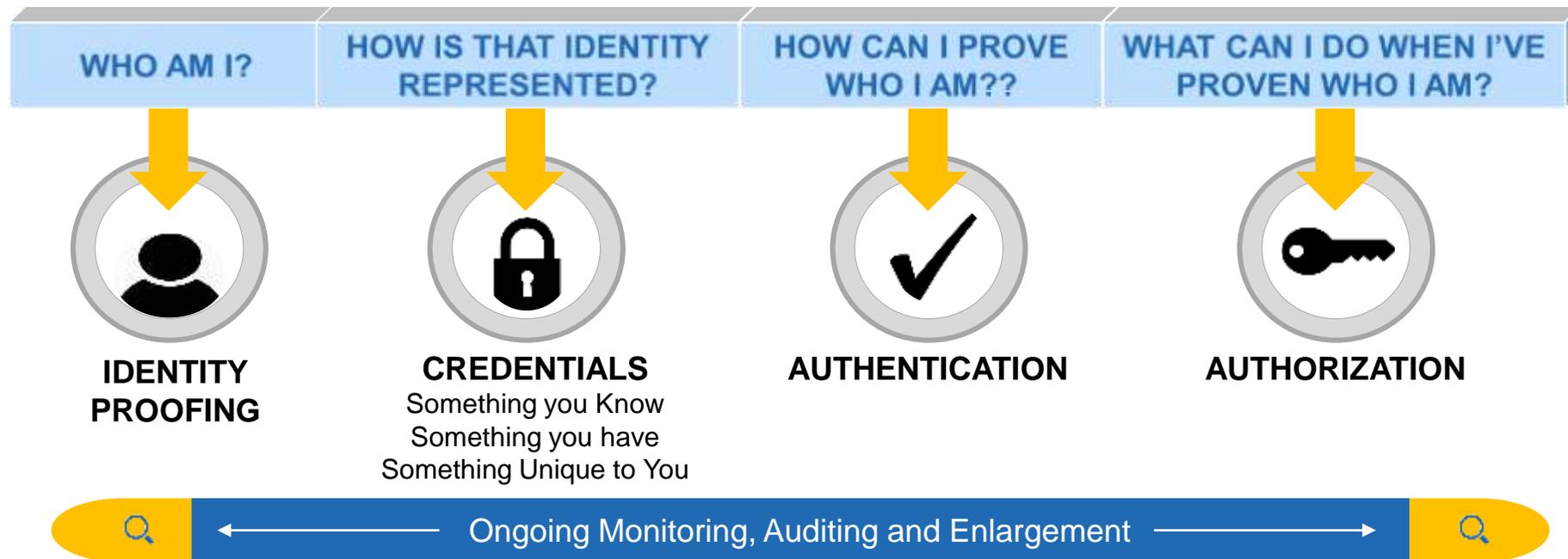
MIFA

“One of the most critical challenge for the healthcare industry is **accurately identifying the patient** and tying that identification to the right designated record set held by a healthcare provider.”

wedi

Verifiable Identity and Authentication of All Participants

Legal requirements and cultural norms dictate that users of systems – whether people or machines – be known so that access to data and services is appropriate. This is a requirement for all participants in nationwide interoperability that supports a learning health system regardless of their role (e.g., individual, patient, provider an administrator)

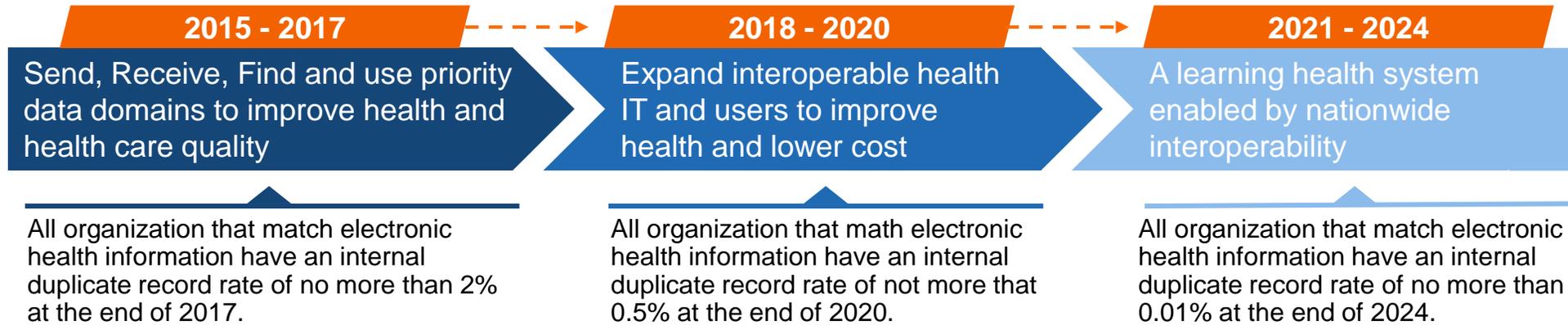


To advance interoperability that enables a learning health system, providers and hospitals need to exchange electronic health information with any other provider or hospital what is appropriately identity proofed and authenticated, especially when directed by an individual to do so.

Source: *Connecting Health and Care for the Nation: A Shared Nationwide Interoperability Roadmap*

We never stand still

Milestone for Accurate Individual Data Matching



Source: *Connecting Health and Care for the Nation: A Shared Nationwide Interoperability Roadmap*

We never stand still

2016 Lenovo Internal. All rights reserved.

Five Steps to Improve Health Safety and Mitigate Financial Risk

- Leverage the following steps to improve data quality, and minimize your financial risk in a value based care delivery model:
 1. Employ an EHNAC accredited Registration Authority (RA) to employ the appropriate processes and protocol to effectively identity proof a patient prior to receiving services which establishes a high confidence in the asserted identity's validity. The ONC recommends that NIST Level-of-Assurance (LoA) 3 criteria for in-person proofing. Note: admittedly doing this in an EMS or Emergency Room setting may not be possible.
 2. Provide associated training to registrars to perform this critical function; best reference for this process would be via a Trusted Agent recognized by the RA – such a person affiliated with EPCS or Direct Messaging (from Meaningful Use Stage 2) and/or the National Association of Healthcare Access Management (NAHAM) should be solicited for this effort.
 3. Assign an UHSI to a patient once they have been properly identity-proofed
 4. Assign the UHSI to a patient record;
 5. Capture a second factor authentication to establish a token to be used across any supporting system. Multiple tokens (based on the approach of a given facility) can be linked to a single UHSI.

AIMexchange: A National Standard

- EHNAC Accredited Registration Authority - Identity Proofing NIST LoA 3
- Standardized Identity Proofing training via NAHAM – each supporting Clinical location established as an accreditation agent
- Establishes a Master Record profiling each unique identity coupled with a Unique Health Safety Identifier (UHSI) and token (ex: credit card, biometric, 4 digit PIN, smartphone)
- Attaches the UHSI to medical record
- Works across all Health IT Systems
- Permits the ability to use the same identity at any supporting AIMexchange clinical location



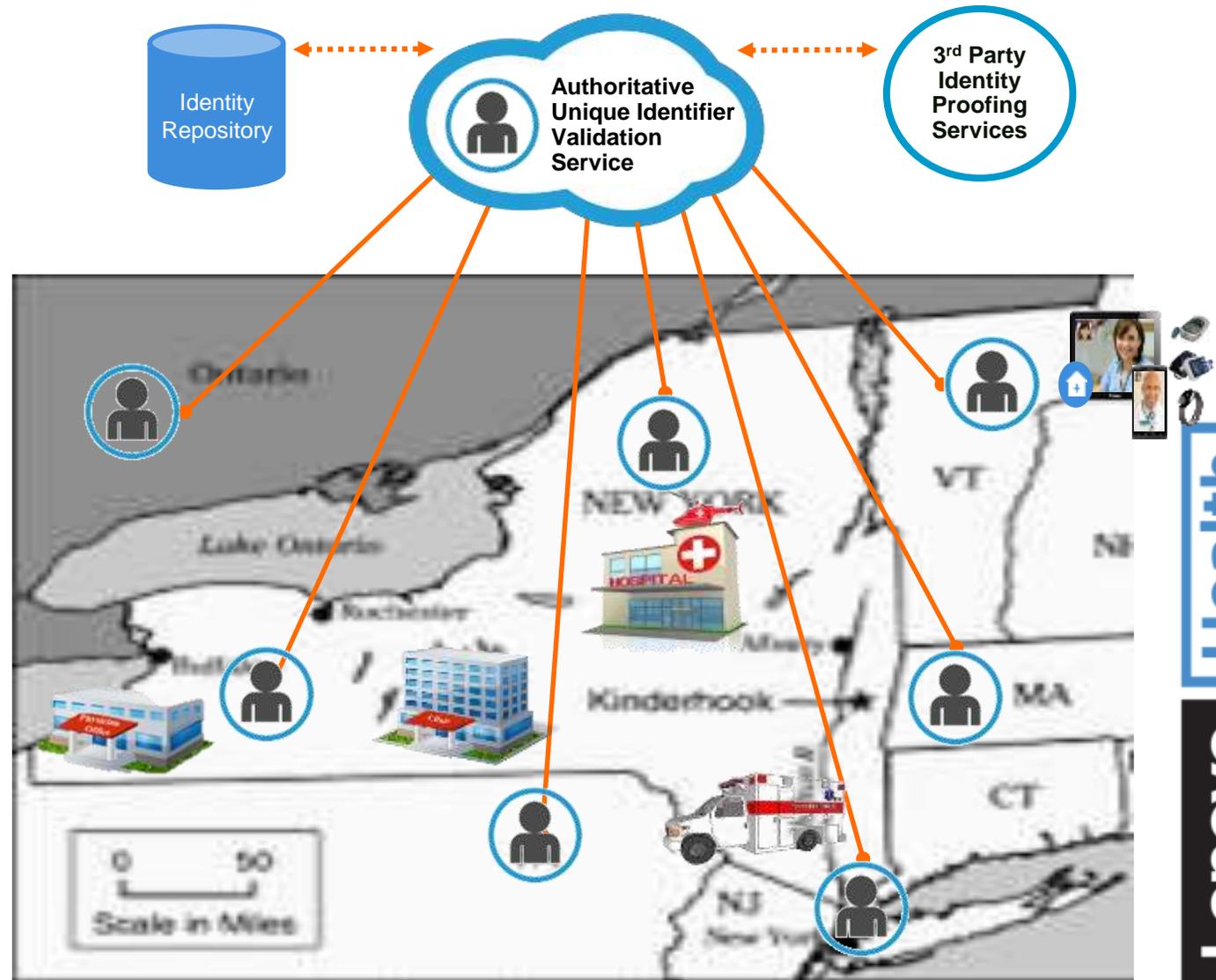
AIMexchange: A National Standard

- EHNAC Accredited Registration Authority - Identity Proofing NIST LoA 3
- Standardized Identity Proofing training via NAHAM – each supporting Clinical location established as a credentialing agent
- Establishes a Master Record profiling each unique identity coupled with a Unique Health Safety Identifier (UHSI) and token (ex: credit card, biometric, 4 digit PIN, smartphone)
- Attaches the UHSI to medical record
- Works across all Health IT Systems
- Permits the ability to use the same identity at any supporting AIMexchange clinical location



Framework to Authenticate Patient Identifier

- EHNAC Accredited Registration Authority - Identity Proofing NIST LoA 3
- Standardized Identity Proofing training via NAHAM – each supporting Clinical location established as an accreditation agent
- Establishes a Master Record profiling each unique identity coupled with a Unique Health Safety Identifier (UHSI) and token (ex: credit card, biometric, 4 digit PIN, smartphone)
- Attaches the UHSI to medical record
- Works across all Health IT Systems
- Permits the ability to use the same identity at any supporting AIMexchange clinical location



Solution Case Study



What We Did

- Mid Coast Hospital employed AIMexchange at the main hospital and 23 clinics within our network
- AIMexchange solution works as the front-end application for our registration staff, enabling them to utilize one platform to speak to the disparate EMR systems
- A branded smart card was chosen for Mid Coast's identity token
- The identity token is matched to a patient record to automatically bring up the patient's medical information
- Check insurance eligibility

What Was Achieved

- Claims denial rate was reduced by 8%
- Average admission time reduced by 75%
- Seamlessly supported an unanticipated increase of 30-40% of patient volumes without investment in additional staff during a merger in 2015
- Repurposed Collection of Payments team from 8 to 1 FTE by prompting outstanding balances at the point of service
- AIMe solution eliminated the creation of duplicate and overlay records.
- High adoption with an average of 500 smart cards being issued daily during product launch
- Over 35,000 cards in circulation

Benefits

Potential Operational Value

	Annual Visits					
	25,000	50,000	100,000	250,000	350,000	500,000
Estimated Annual Value as a Result of Improved Data Quality	\$56,334	\$75,084	\$112,584	\$225,084	\$300,084	\$412,584
Potential Estimated Annual Patient Access Staff Cost Savings for Data Collection and Verification Activities	\$86,666	\$173,333	\$346,667	\$866,667	\$1,213,333	\$1,733,333
Potential Estimated Annual Patient Access Staff Cost Saving for Financial Clearance Time (Estimation, Collection)	\$44,236	\$88,472	\$176,944	\$442,361	\$619,306	\$884,722
Potential Estimated Annual Savings	\$187,236	\$336,889	\$636,195	\$1,534,112	\$2,132,723	\$3,030,639

Potential Annual Savings are based upon industry averages

- Improved Data Quality
- Reduction of Clinical Errors Due to Inaccurate or incomplete Health Records
- Reduction of Duplicate Test
- Better Outcomes
- Improved Patient Experience

Thank You!

LenovoHealth: Customize Care Anywhere



Andy Nieto
Health Solutions Executive

LenovoHealth

www.lenovohealth.com

O: 919.294.1183

C: 502.905.0230

E: anieto1@lenovo.com

T: @ALN996