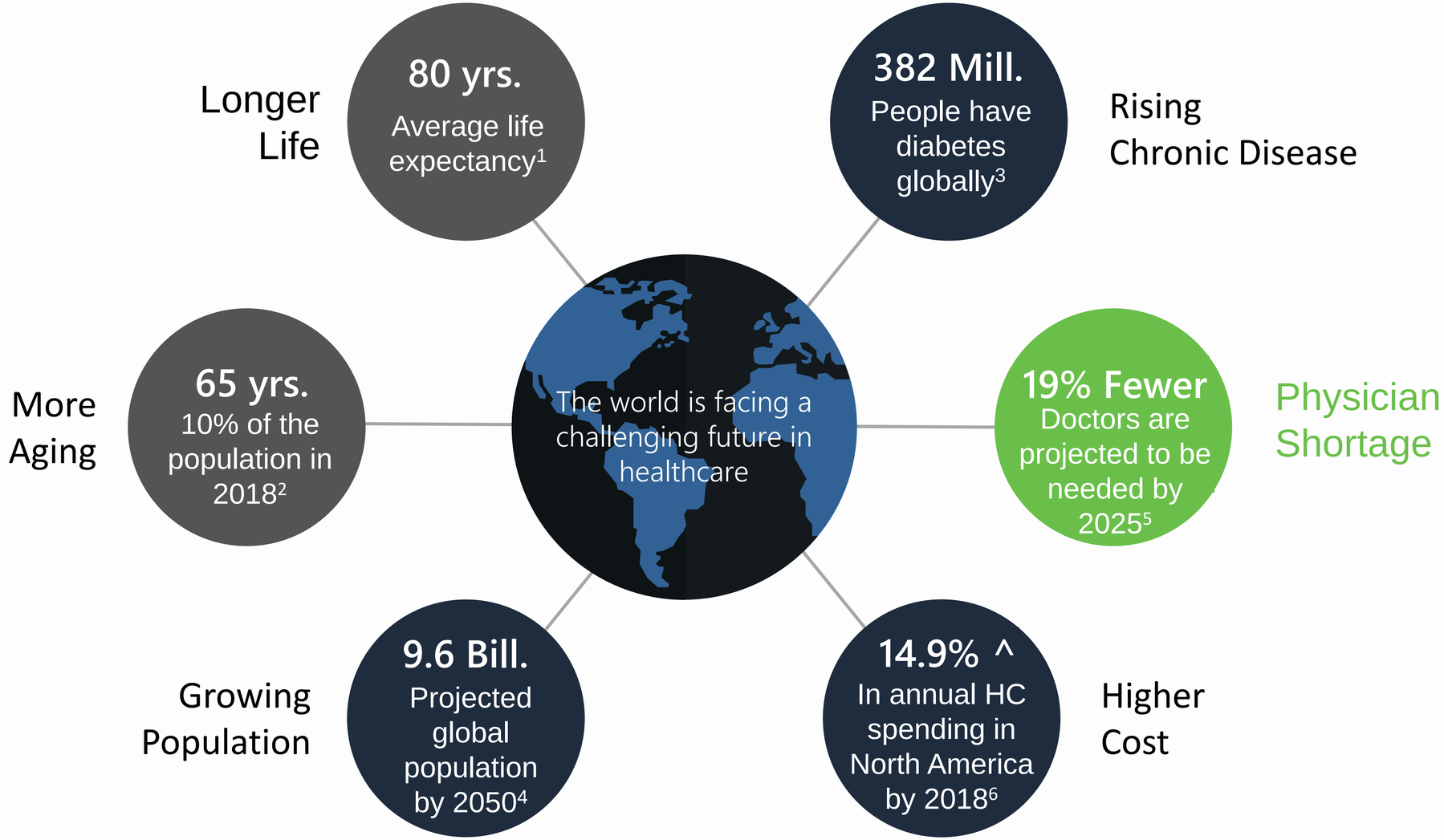
Enhancing Data Integrity w/ Unique Health Safety Identifier

Tom Foley
Director, WW Health Solution Strategy
LenovoHealth

MACRO TRENDS



Source: 1: Life expectancy data, World Health Organization, 2012; 2: Global life sciences outlook, Deloitte, 2014; 3: American Association Medical College, 2010; 4: UN population projections

HEALTH PLUS CARE TRANSFORMATION

Clinical Integration

Today:

Reactive and Volume-based

The Future:

Proactive and Value-based

Consumer Engagement

Awareness

Wellness

Healthcare IT News

Government & Policy

Industry groups press Congress to back private-sector patient matching solutions

HIMSS and 24 other organizations want the feds to support creating unique patient identifiers to improve care delivery.

By Bill SiwickiApril 10, 2017 01:14 PM

…“For nearly two decades, **innovation and industry progress has been stifled** due to a narrow interpretation of the language included in Labor-H bills since FY1999, prohibiting the Department of Health and Human Services from adopting or implementing a unique patient identifier,”…

THE WORLD OF INTEROPERABILITY

Disparate systems have a large impact on HCO's ability to accurately share patient data

ENTERPRISE MASTER PATIENT INDEX

The limitations of an enterprise master patient index

Historical 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.

PROBLEMS

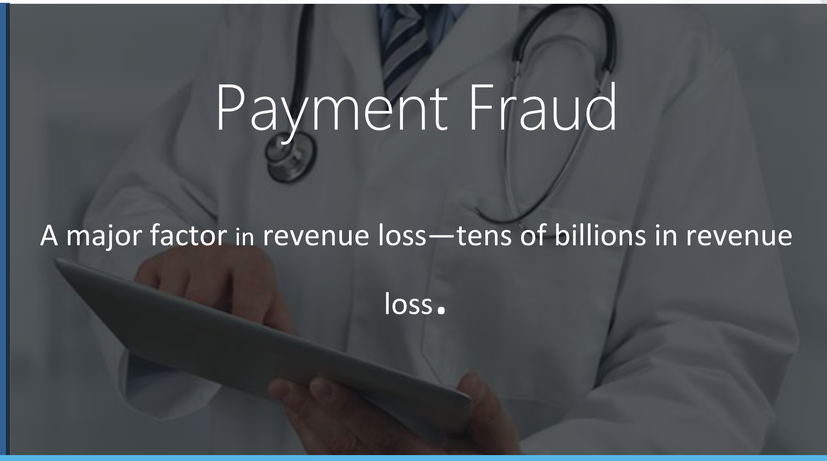
Do these challenges impact your clinical and financial operations?

Duplicate Records

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

Medical Identity Theft

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



Payment Fraud

A major factor in revenue loss—tens of billions in revenue loss.

Securing Data Integrity

- On average, an excess of 12% of medical records are duplicates [1]
- ONC's objective is to reduce that rate down to 2% by 2017, 0.5% by 2020, and 0.1% by 2024 [2]

- Costs the United States $84 billion annually [3]
- In 2014, medical identity theft victims paid $20 million out-of-pocket [4]

- $272 billion is lost to Medicare and Medicaid fraud and abuse [5]
- 62% of finance professionals report that their organization were targets of payment fraud in 2014. This has translated to nearly $28 Billion in overall cost [6]

CHALLENGE SUMMARY

Medical identity theft, duplicate records & fraud have been *long standing problems* in the care delivery model

Securing Data Integrity

- If patient authentication (i.e. biometrics) is already in place at check in, it is commonly not paired with industry recommended identity proofing processes
- If healthcare networks have implemented data reconciliation processes (MDM, EMPI), records may be merged without the awareness or detection inaccurate or faulty data
- If identity proofing occurs it is often not linked with a universal identifier that can be utilized across the continuum of care

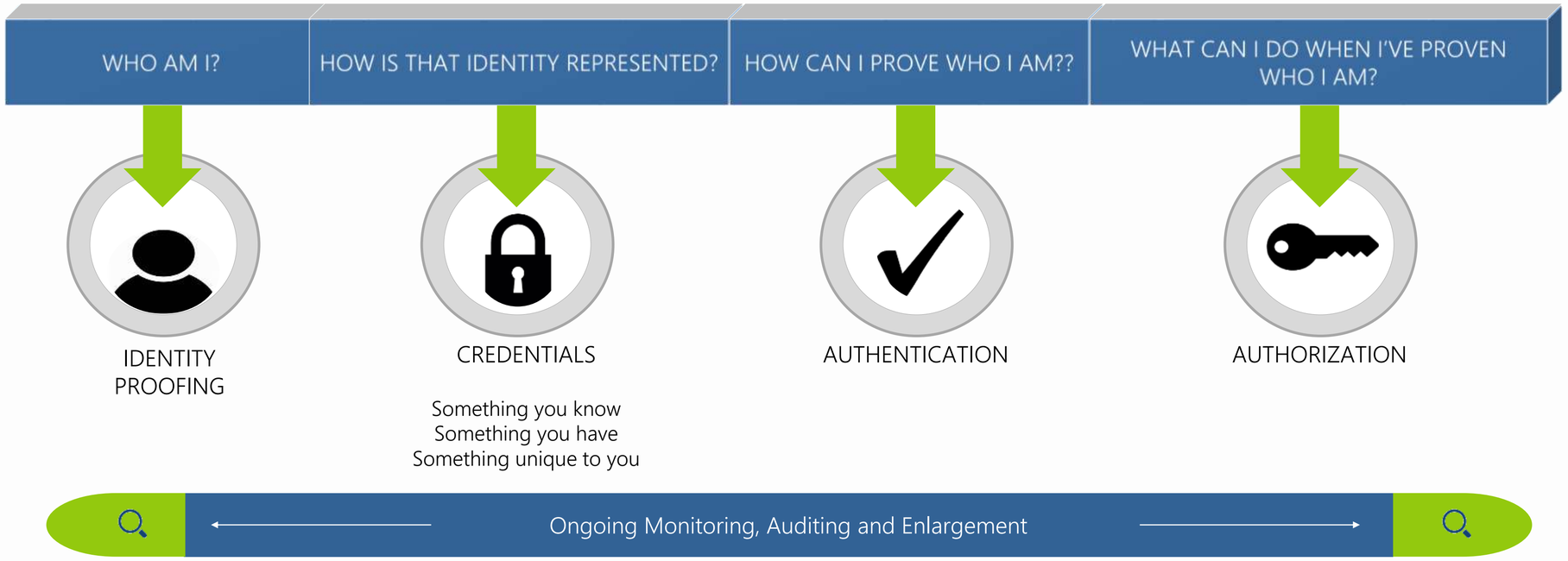
360 SECURITY

- 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.
- Information about a person vs Identity Credentials
  - Driver's licenses, SSNs, birth certificates and other forms of information which represents an individual were not intended to be identity credentials
  - As a result of the many noted data beaches the acquired information is making its way into the mainstream as synthetic identities.
    - Therefore it's challenging to confirm that the presenter of credential(s) is the individual they are claiming to be.
  - Hence the importance of enhancing the health services registration process with a strong identity proofing process coupled with collecting and validating the representation of the person with a biometric or other secure and precise authenticator.

ONC RECOMMENDATIONS

Verifiable identity and authentication of everyone

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. [1]

ONC MILESTONES

Accurate data matching for healthcare facilities

Improve Safety and Mitigate Risk

The five steps in correlation with the ONC

Easily leverage the following steps to improve data quality, and minimize your financial risk in a value based care delivery model:

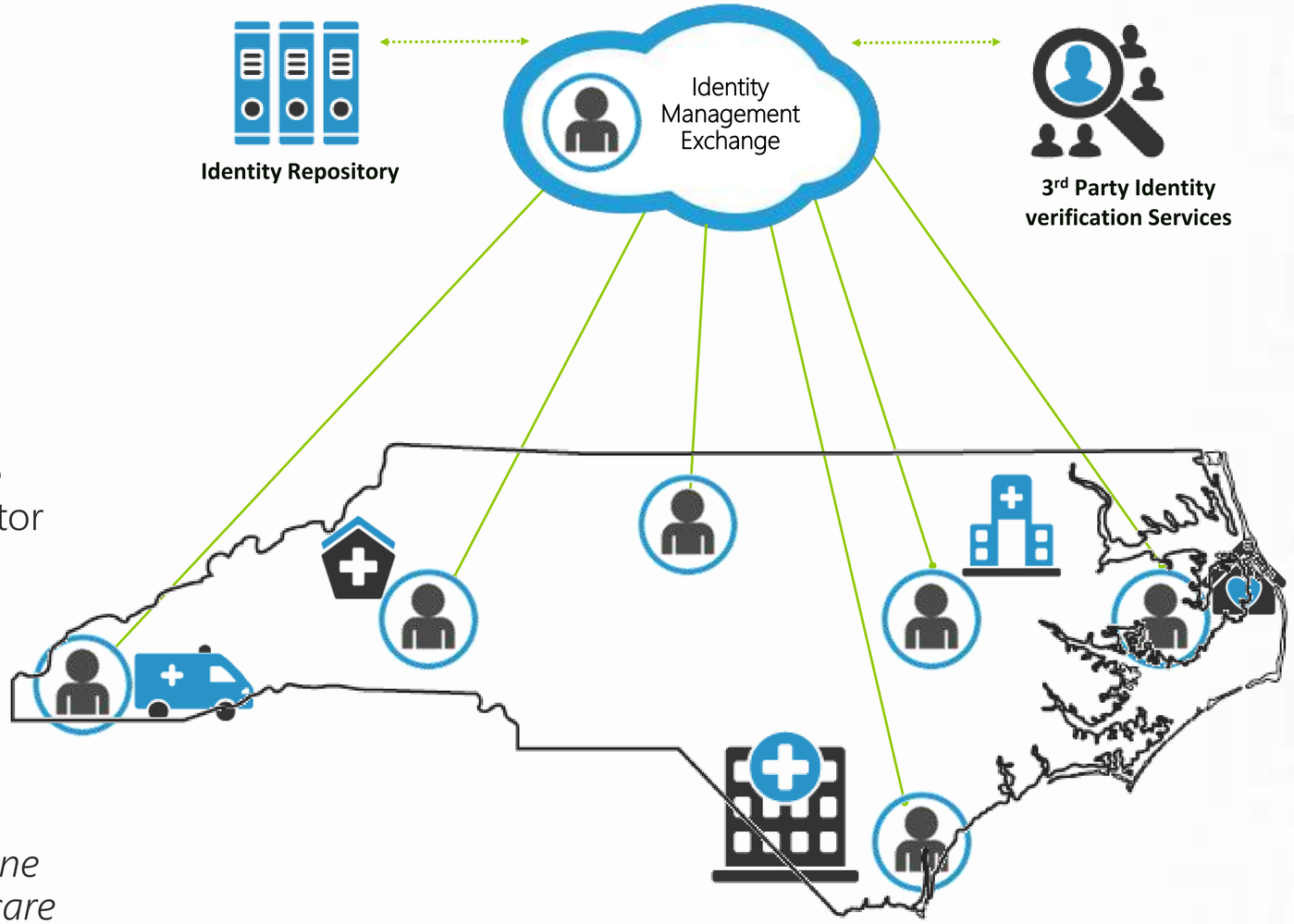
1. Adopt accredited protocol to effectively identity proof a patients to establish a high confidence in the asserted identity. The ONC recommends that NIST Level-of-Assurance (LoA) 3 criteria for in-person proofing. *Note: this may not be possible EMS or Emergency Room settings or for other patient-specific situations.*
2. Provide training to registrars to perform the critical function outlined in step 1. A Trusted Agent, or registration specialist, that is affiliated with EPCS or Direct Messaging (from Meaningful Use Stage 2), and/or NAHAM should be solicited for this effort.
3. Assign an Unique Health Safety Identifier (UHSI) to a patient once they have been properly identity-proofed.
4. Link the UHSI to that patient's record(s).
5. Establish a token with second factor authentication (2FA) to be used across any supporting system. Multiple tokens (based on the approach of a given facility) can be linked to a single UHSI.

ALIGNING WITH STANDARDS

UHSI improve health safety and mitigate risk

- Strong Identity Proofing within ONC Recommendations – NIST LoA3
- Standardized Identity Proofing training via NAHAM
- Establishes a interoperable "Master Record": providing each unique patient with a Unique Health Safety Identifier (UHSI) with multi-factor authentication via a "token" (ex: credit card, biometric, smartphone)
- Links the UHSI to patient's medical record(s)

The patient's verified identity is supported at any AIMe clinical location – establishing one patient, one identity and one record across the continuum of care regardless of the EHR



The North Carolina representation is an example of a connected care model and can correlate to any state or nation-wide solution

ONE PATIENT, ONE IDENTITY, ONE RECORD

Why it matters

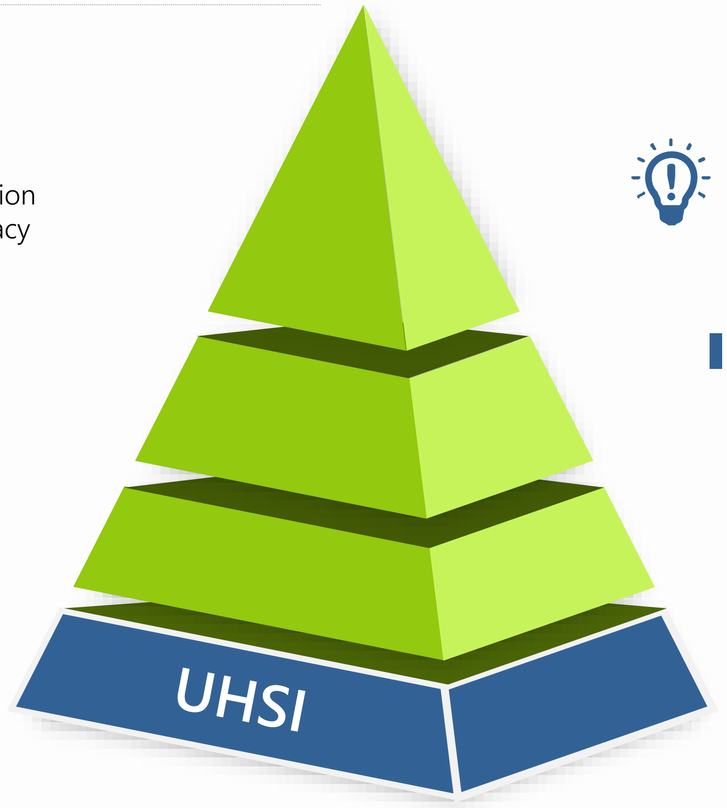
Establishing a solid identification foundation that eliminates errors and delivers accuracy

Healthcare Pyramid

3 Big HC Initiatives

2 Existing Systems

1 Identity Foundation



Value-Based, Patient-Centric Care

Metrics and Payment

Reliable Record Access

EHR & EMPI with Trusted, Interoperable UHSI

Accurate Identification is the foundational component in achieving national health strategies

Patient safety

is increased

Check in

is streamlined automated

PII Data

is reliable

Record Matching

is accurately achievable

Security

from walk-in to payment

Reliable Record Access

- Increased experience/satisfaction via automation and validation
  - Patient
  - Registration Clerk
- Increased patient safety

Metrics and Payment

- Government reimbursement
- Billing: Expedited and accurate Co-Pay and Outstanding Balance Collections
- Accurate patient counting (via accuracy in denominators) and reporting

Value-Based, Patient-Centric Care

- Meaningful Use
- HITECH
- Pop Health
- ACO
- Continuity of Care
- Interoperability
- Others

EHR & EMPI with Trusted, Interoperable Unique Health Safety Identifier

Lenovo Health

UHSI drives:

Patient Idenity

One patient

Establish Identity of your patients

Record Link

One record

Link UHSI to the patient's correct medical record

Record Invoke

Every time

Automatically invoke a patients medical record

Interoperable across all settings of care – regardless of EHR

Thomas Foley
Director, WW Health Solution Strategy

919-697-4152

tfoley@Lenovo.com